

# State of Washington

## *General*

*Code:* S1Washington-FS24  
*Name:* State of Washington  
*Group:* Financial Audit  
*Type:* S1-Agency, Commission, or Board  
*Location:* State  
*Scope:* Not Applicable

## *Team*

*Lead:* Rajpreet maynock  
*Manager:* Steven Wendling

## Procedures

### D.1.PRG - Taxes Receivables (Net of Allowance)

*Procedure Step:* Summary & Conclusion  
*Prepared By:* BFW, 10/8/2024  
*Reviewed By:* CJG, 11/21/2024

Purpose/Conclusion.*
----------------------

**Purpose:**

# State of Washington

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

## **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

## Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

## State of Washington

- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

# State of Washington

## Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **D.1.PRG - Taxes Receivables (Net of Allowance)**

*Procedure Step:* Understanding of Line Item

*Prepared By:* BFW, 5/21/2024

*Reviewed By:* SHW, 7/31/2024

## Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**



## State of Washington

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associated with the line item.
- Evaluate trends to identify:
  - (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
  - (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
  - (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

# State of Washington

Guidance/Criteria:

Record of Work Done:

**(1) Prior Audit Exceptions:**

There were no prior year audit exceptions for this balance.

**(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

The Taxes Receivable (Net of Allowance) balance is the result of debit entries for year-end accrued and unavailable revenues (non-current) and is comprised primarily of the following taxes:

- Property taxes
- Retail sales taxes
- Business and Occupation taxes

Receivable balances are determined using the Automated Tax and Licensing Administration System (ATLAS). We met with Ayano Faasumalie, Revenue & Financial Reporting Coordinator, on April 10, 2024 to gain an understanding of receivable types in ATLAS and the applicable calculation for allowance for uncollectibles. She explained the types of receivables and calculation related to allowance for uncollectibles remains the same since the implementation of ATLAS in FY19. See the table below:

Receivable Type	Allowance Methodology
Return Receivables	Accounts in Deferred Status (Actual Amounts)
Estimated Returns	Discount Rate applied to locked returns; collection rate applied to unlocked returns to determine accrued revenue versus unavailable revenue
Audit Receivables	Uncollectible Allowance rate applied at FYE, determined from real time adjustments to audit receivables during FY
Lien Receivables	Lien accounts in deferred status (Actual amounts) plus additional allowance rate applied at FYE

## State of Washington

To determine how to apply the uncollectible rate to the different receivable types, DOR analyzes how much was moved into Deferred Status for each receivable type during the fiscal year. Based on this analysis performed by DOR, it was determined that return receivables and estimated receivables in deferred status do not need the uncollectible rate applied to them. Only the actual balance due amounts on the taxpayer accounts that are in Deferred Status for each of those receivable types will be recorded in Allowance for Uncollectibles.

It was also determined that Lien Receivables have a higher percentage of accounts that moved into Deferred status; therefore, DOR applies a 5 year average of a lien uncollectible rate to the Lien receivables. The amount recorded into Allowance for Uncollectibles for the Liens receivables is the uncollectible rate multiplied by the lien receivable balance and any taxpayers' accounts in deferred status. Additionally, an analysis of audit receivables was performed to determine what real dollar adjustments had been made to audit receivables for the year and an uncollectible rate was determined and applied for those accounts. The total adjustments and write-offs for audit receivables are divided by the beginning balance for audit receivables to determine the uncollectible rate to be applied. During testing, we will review the methodology that DOR uses to estimate uncollectible taxes for the Allowance for Uncollectibles amount.

Changes noted by DOR:

We requested Internal Audit's risk assessment related to revenues and receivables from Sandi Fairchild, Chief Financial Officer, to identify any significant changes to note for the taxes receivable balance. During our review, we did not note any changes in the composition or reporting of the taxes receivable balance. We inquired with Ayano who stated processes have remained the same for identifying and reporting taxes receivable. **No significant changes or risks identified.**

### **(3) Updates to Significant Account Matrix:**

We identified no changes that need to be made to the Significant Account Matrix.

### **D.1.PRG - Taxes Receivables (Net of Allowance)**

*Procedure Step:* Controls - ATLAS

*Prepared By:* BFW, 6/20/2024

*Reviewed By:* RKM, 10/11/2024

Purpose/Conclusion:
---------------------

**Purpose:**

# State of Washington

To gain an understanding of internal controls.

## **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

## **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

## State of Washington

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

# State of Washington

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls in the Automated Tax and Licensing Administration System (ATLAS) address the following balance(s):

- **Taxes Receivable (Net of Allowance)** - General Fund
- **Taxes Receivable (Net of Allowance)** - Government Activities

For the following assertions:

- **Existence** - There is a risk that recorded receivables are less than source records.
- **Valuation** - There is a risk that taxes receivables are incorrectly computed. There is a risk that the allowance is incorrectly estimated.
- **Completeness** - There is of incorrect timing of revenue recognition resulting in an under-accrual of revenue.

## **Gain an Understanding of Internal Controls**

We met with Ayano Faasumalie, Revenue & Financial Reporting Coordinator, in Business & Financial Services (B&FS) and Sandi Fairchild, CFO, on April 10, 2024 to gain an understanding of taxes receivable.

## **Background:**

### **Automated Tax and Licensing Administration System (ATLAS):**

Implemented on March 19, 2018, ATLAS replaced all of the Department’s legacy systems specific to taxpayer administration including the receivables system, TARIS. ATLAS is driven by the taxpayer return, which the majority of taxpayers file on-line through MYDOR, part of the State's SecureAccess Washington (SAW) single sign-on application gateway. This was created by the Washington State Department of Information

## State of Washington

Services (which in 2011 became part of Department of Enterprise Services) to simplify access to a list of government services accessible via the Internet. ATLAS's automated tax return form is hard coded with the appropriate codes for each of the tax types so the fund, tax revenue source, general ledger codes, etc. is properly recorded. Active taxpayers are required to submit returns either monthly, quarterly, or annually as determined by Taxpayer Account Administration Division.

The following are the four different types of receivables identified within ATLAS:

- **Return Receivables:** Tax returns submitted by taxpayers without payment or with partial payment leaving a balance due. ATLAS automatically records a return receivable (balance due) in the taxpayer's account the next day after the due date.
- **Audit Receivables:** Based on an assessment from an auditor. When the auditor identifies an adjustment is needed, a tax return in the system is posted to the taxpayer's account and becomes a receivable the next day.
- **Estimated Return Receivables:** Results from estimated tax returns for businesses that have failed to file a tax return on time. The system identifies an account that was expected to file a tax return and was not filed by the due date. ATLAS will automatically create a return, which estimates the amount of tax due based on up to 4 years prior filing history from the taxpayer's account or industry standards if the taxpayer does not have 4 years of history. This amount is multiplied by the hard coded tax rates in ATLAS to determine the amount due. The estimated return is posted to the taxpayer's account in ATLAS. The system will automatically put a CAS - HOLD (called "locked") on the estimated return so that the taxpayer will not be able to view the estimated amount. Locked returns are not recorded as a receivable until a Compliance Agent has reviewed the estimated return for reasonableness (or the business has paid the balance). Since the Agent is familiar with the taxpayer, the Agent may make adjustments to the estimated amount if deemed necessary. Changes are reviewed by a Supervisor. Once the Compliance Agent's review is completed, they will release/unlock the Hold and the estimated return amount will then be recorded as a receivable (and viewable by the taxpayer in their account).
- **Lien Receivables:** These were called Warrants, which result from Return, Estimated Returns, and Audit receivables that have had unsuccessful collection efforts. A taxpayer's delinquent account goes through a compliance assessment. All receivable types (Audit, Estimated, & Returns) for that taxpayer are assumed into one lien receivable. The lien (warrant) is filed in district court as a lien against the taxpayer's business. Once the lien is filed, it is in effect for 10 years, or until the outstanding balance is paid in full and DOR takes the lien off the property.

### **Calculation and Identification of Excise Tax Receivable:**

The monthly process of recording taxes receivable begins with tax returns that are overdue or underpaid. When a tax return is entered into ATLAS, the system will automatically review the tax return, looking for variances using built-in parameters for calculations and logic statements in order to flag errors or high risk items, including returns that do not have a payment or the payment does not match the return amount. Work items are created for returns that do not automatically post to a taxpayer's account in ATLAS until it is reviewed by a Taxpayer Account Administration (TAA) Examiner. If there is a balance due on the return, ATLAS will automatically create a receivable including penalties and interest based on the due date, which is automatically posted by ATLAS in the taxpayer account (**Key Control #1 – Automated – Completeness/Valuation**). If a tax return was not filed by the due date, ATLAS will automatically create an estimated tax return one week after the due date based on the account's reporting history, (or with specific amounts based on reporting frequency if the taxpayer has no past

## State of Washington

reporting), then multiply those amounts by the hard coded tax rates. Accounts in locked status are not posted until reviewed for reasonableness by Compliance Agents.

### **Calculations of Rates and Adjustments**

The process of determining the fiscal year-end taxes receivable balance includes the application of a discount rate, uncollectible rate, and accounts in deferred status to provide a reasonable estimate of the taxes receivable balance that will be collected. Therefore, Taxes Receivable is recorded in the financial statements net of the following three different types of adjustments:

**1. Discount Rates:** Discounts are an estimated amount that is based on the assumption that receivables have been overstated. The discount rate reduces the receivable amount but is not recorded in the Allowance for Uncollectible. Currently, the only receivable type considered by DOR to be overstated is the locked estimated return receivables and will have a discount rate applied to those receivables. DOR decided to discount the locked estimated returns because in some instances a business may have closed or had no activity in ATLAS during the period.

DOR performs an analysis to determine how much of the locked estimated returns at fiscal year end (FYE) were actual receivables. To calculate the discount rate, the actual receivables is divided by the total locked estimated returns at FYE. The remaining locked returns as of FYE have not been reviewed and are therefore, still locked at the end of the fiscal year. Also, additional estimated returns were generated by ATLAS during the current fiscal year. The discount rate is manually applied to the balance of the locked estimated returns when a Journal Voucher (JV) is created to record the Taxes Receivables for FYE estimated return receivables.

For all other receivable types (Audit, Returns, and Liens) DOR decided the other receivable types' balances are not overstated and are actual receivables; therefore, a discount rate is not applied.

**2. Uncollectible Rates:** DOR changed this methodology based on a discussion with OFM in FY19 and the process has remained the same since then. DOR's analysis showed that a low percentage of accounts were put into deferred status during FY19; therefore, the uncollectible rates are not applied to return receivables or estimated return receivables. For these receivable types, only taxpayer accounts in deferred status would be recorded into Allowance for Uncollectible, see below in #3. For lien receivables, taxpayer accounts in deferred status and estimated uncollectible amount are recorded in Allowance for Uncollectible. Audit receivables have an estimated uncollectible amount recorded in Allowance for Uncollectible based on an uncollectible rate.

**3. Accounts in Deferred Status:** Compliance is responsible for collecting the receivables from all revenue sources. When Compliance has exhausted their collection efforts, or it is not cost effective to continue, the account is put into deferred (or uncollectible) status. DOR analyzed how much was moved into Deferred Status for each receivable type during the year. Based on this analysis, DOR decided that due to the low percentage of accounts moved into deferred status for return receivables and estimated receivables, they will not have an uncollectible rate applied to them. Only the actual balance due amounts on the taxpayer accounts that are in Deferred Status for each of those receivable types will be recorded in Allowance for Uncollectible.



## State of Washington

DOR determined that Lien Receivables have a higher percentage of accounts that moved into Deferred status in the fiscal year; therefore, DOR applied a 5 year average of a lien uncollectible rate to the Lien receivables. The amount recorded into Allowance for Uncollectible for the Liens receivables is the uncollectible rate multiplied by the lien receivable balance and any taxpayers' accounts in deferred status. Additionally, an analysis of audit receivables was performed for FY19 to determine what real dollar adjustments had been made to audit receivables for the year and an uncollectible rate was determined and applied for those accounts. The total adjustments and write-offs during the fiscal year for audit receivables was divided by the beginning balance for audit receivables to determine the uncollectible rate to be applied. Ayano explained that DOR has maintained this process since the analysis performed in FY19.

Business & Financial Services recalculates rates and tests the rates (discount, collection and uncollectible) for accuracy.

### **How transactions are recorded in AFRS:**

#### **Monthly Journal Entries**

On the last business day of the month, ATLAS automatically prepares and posts Journal Vouchers (JV) by revenue source and receivable type to record the taxes receivable, accrued revenue, deferred inflows, and the allowance for uncollectible as well as interest and penalties (**Key Control #2 - Automated Interface – Existence**). Depending on the type of receivable, the allowance for uncollectible is calculated differently based on the analysis above. See summary of analysis in the table below:

<b>Receivable Type</b>	<b>Allowance Methodology</b>
Return Receivables	Reduced by Accounts in Deferred Status (Actual Amounts)
Estimated Returns	Discount Rate is applied to locked returns; collection rate applied to unlocked returns to determine accrued revenue versus deferred inflows
Audit Receivables	Reduced by Uncollectible Allowance rate applied at FYE, determined from real time adjustments to audit receivables during FY
Lien Receivables	Reduced by Lien accounts in deferred status (Actual amounts) plus additional allowance rate applied at FYE

After ATLAS prepares the JV, Revenue Accounting has 6 business days to review the JV before it is automatically released by ATLAS into AFRS to record the JV; this happens in ATLAS on the 6th business day. On the 7th business day of the following month, Revenue Accounting can see the JV in AFRS. ATLAS is able to separate out taxes receivable that relate to the dedicated funds and enter the taxes receivables directly into these funds instead of into Fund 001 - General Fund. The JV is recorded as a monthly balance, therefore ATLAS generates reversal JVs for the prior month's tax receivable JV amounts.

# State of Washington

## **Year End Gross Receipts Journal Entry**

This same process is performed at fiscal year-end (FYE) to record accrued and deferred inflows except for the Gross Receivables. To record the Gross Receivables at FYE, for monthly filers, excise tax returns for June activity are due July 25th and for quarterly filers, tax returns for the 4th fiscal quarter (April, May, and June) are due July 31st. In August, the ATLAS "gross receipts" report, which is programmed to pull all gross receipts for the period July 1-August 15, is downloaded to Excel and compared to the gross receipts from the prior five years to check that the values seem reasonable. Revenue Accounting will reconcile and review the year end JV to enter into AFRS to show the June returns received after June 30<sup>th</sup> as a receivable and accrued revenue for the FYE (**Key Control #3 - Manual - Existence/Completeness**).

## **Monthly ATLAS to AFRS reconciliation:**

At the end of each month, a reconciliation is performed by Revenue Accounting between ATLAS and AFRS to ensure all of the monthly revenue activity has been properly posted to AFRS. Andrew Arnold, Revenue Accounting Supervisor, runs a customized WebI report for taxes received during the month recorded in AFRS. Revenue Accounting will also run a monthly revenue activity report that includes receivables and revenues from all taxes. Most tax revenues are from ATLAS with the exception of property tax in Property Tax Receivable System (PTRS) and taxes recorded in the Cash Receipts Reporting System. Revenue Accounting uses an Excel worksheet to reconcile reports from Webi and ATLAS (**Key Control #4 - Manual - Existence/Completeness**).

To specifically review receivable and allowance for uncollectible balances, Alison Walker, one of Ayano's employees from the Financial Reporting & Systems Support team, pulls a monthly ATLAS report (by receivable type) into a spreadsheet and compares the Discounted receivables balance month-to-month and the Uncollectibles month to month comparison to prior months in the same FY for anomalies (**Key Control 5 - Existence/Valuation**). The comparison is done to ensure the allowance methodology described above is applied consistently. Any anomalies are investigated, and explanations are provided at the bottom of the worksheet with links to the source of the anomaly for easy investigation. There is no minimum threshold for an anomaly investigation.

## **Write Offs:**

By statute [RCW 82.32.340](#), tax debt is never "forgiven" until it is legally written off. The process is as follows:

The uncollectible write-off can be performed at any time by the Warrant Team Tax Administration Manager (TAM). The Adjustments report is generated in ATLAS. The report is generally ran twice a year.

The 12 year write-off report selection criteria (bill due transaction is 12 years or older with open balance):

1. No active liens. If there is a linked liability (TFAAs and successorships) or multiple taxpayers in a lien, the write off process evaluates each taxpayer separately.
2. The collection has to be in deferred stage (linked collections w/o deferred stages are excluded)
3. No payments within the last 2 years
4. No taxpayers with open adjustment requests

## State of Washington

A Prevent Write Off indicator is placed on the account if the taxpayer is paying restitution. The Warrant Team TAM and Excise Tax Examiner (ETE) 3s review the report and can Reject pending write-off adjustments if it is determined that an account should be removed from the list.

The Warrant TAM runs the 12 year write off request job stream in the production environment. This happens on a Friday, so the report will appear in the staging environment on Monday. After the report is reviewed by the TAM and the Warrant Team ETE3s, a 12 year write off approval job is completed in Staging. The Warrant TAM will then run a discrepancy report between the original request and approved request. This report is called Adjustments – Differences. After the report is reviewed and the write off report is adjusted; the Warrant TAM will run the 12 year write off approval job stream in Production. This will post and approve all the pending transactions based on the indicators and changes made in the real production environment.

### **Key controls are as follows:**

- **Key Control #1 – Automated – Completeness/Valuation** – ATLAS will automatically create a receivable including penalties and interest based on the due date, which is automatically posted by ATLAS in the taxpayer account. If a tax return was not filed by the due date, the day after the due date ATLAS will automatically create an estimated tax return based on the account's reporting history and tax rates.
- **Key Control #2 – Automated – Existence** – On the last business day of the month, ATLAS automatically prepares and posts Journal Vouchers (JV) by revenue source and receivable type to record the taxes receivable, accrued revenue, deferred inflows, and the allowance for uncollectible.
- **Key Control #3 - Manual - Existence/Completeness** - In August, the ATLAS "gross receipts" report, which is programmed to pull all gross receipts for the period July 1-August 15, is downloaded to Excel and compared to the gross receipts from the prior five years to check that the values seem reasonable. Revenue Accounting will reconcile and review the year end JV to enter into AFRS to show the June returns received after June 30<sup>th</sup> as a receivable and accrued revenue for the FYE.
- **Key Control #4 - Manual - Existence/Completeness** - At the end of each month, Revenue Accounting runs a revenue activity report (MRA) from ATLAS and downloads AFRS revenue and receivable data from Enterprise Reporting into Excel. A reconciliation is then performed between ATLAS and AFRS to ensure the reported revenue and receivable amounts are accurate and complete.
- **Key Control #5 - Manual - Existence/Valuation** - Financial Reporting & Systems Support pulls monthly ATLAS report (by receivable type) into a spreadsheet and compares prior months (in same FY) reviewing for anomalies in the receivables and allowance calculations.

### **Noted Weaknesses are as follows:**

None

### **D.1.PRG - Taxes Receivables (Net of Allowance)**

# State of Washington

*Procedure Step:* Key Control #1 (Automated)  
*Prepared By:* BFW, 6/25/2024  
*Reviewed By:* RKM, 8/20/2024

## Purpose/Conclusion:

### **Purpose:**

To determine whether ATLAS calculates the receivable, including penalties and interest (**Key Control 1 for ATLAS**) was in place in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - ATLAS\]](#).

## Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

- Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

- What formulas are used to make the calculation?

## State of Washington

- What values or factors are used to make the calculation? For example:
  - Rate tables used by the calculation
  - Profile fields (i.e., applicable transaction types)
  - Programmed/set formulas and/or values
  - Constraints (i.e., effective date, minimums/maximums, etc.)
- How is the calculation triggered or initiated?
- How is the calculation recorded in the accounting system (or used in an end result)?

### Automated Interfaces:

- Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?
- What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

- Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

- Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

- Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

# State of Washington

## Edit Checks:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?
  - What transactions, data, tasks, or documents are approved?
  - Who are the preparers? How do preparers submit for approval?
  - Who are the authorized approvers? Are there backup approvers?
  - What documents or information are required to make approval judgment?
  - What is the next step once a transaction/data/ task/document is approved or denied?
  - Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?
- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

## Computer Generated Reports:

- What information or exceptions is the report designed to identify (what is the purpose of the report)?
- How is the report used and by whom?
- For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and*

## State of Washington

*follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

- What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?
  - What transactions, data, tasks, or documents are approved?
  - Who are the preparers? How do preparers submit for approval?
  - Who are the authorized approvers? Are there backup approvers?
  - What documents or information are required to make approval judgment?
  - What is the next step once a transaction/data/ task/document is approved or denied?
  - Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?
- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for*

# State of Washington

*overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

- Re-perform the calculation for selected transactions.  
*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*
- *In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*
- If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.  
*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*
- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **Automated Interfaces:**

- Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.  
  
*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*



## State of Washington

*Note: these procedures would also provide substantive evidence.*

- Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

- Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.
- When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

- Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

- For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.
- Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

## State of Washington

- Observe a transaction to see the approval process and verify any key aspects of the process or limits.
- If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### **Software Calculation:**

- Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.
- How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

- What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables*

## State of Washington

*or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

- Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.
- What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*
- How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

## State of Washington

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

- Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.
- How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

- What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

## State of Washington

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

- Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.
- How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

- Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

- If the report is hardcoded into the system, how are program changes made?
- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

- NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

## State of Washington

- How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.
- If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?
- If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Automated Interfaces:

- Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.
- Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Edit Checks:

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

## State of Washington

- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*



## State of Washington

- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

- [Instructions](#) are located in Team IT Audit's System's Sharepoint page.
- Details of IT Security related issues should NOT be included in any emails or helpdesks.
- Exit, ML and Findings should be separately communicated in an IT Security Results Document.
- Findings will be referenced, but not included in the audit report.
- All IT security-related recommendations must be reviewed by [Team IT Audit](#).
- Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Information Technology](#) Planning Guide**

# State of Washington

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

## Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is*

# State of Washington

*initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

- Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.
- Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.
- Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).
- Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.
- Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.
- Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.
- Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.
- Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.
- Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.
- Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

## State of Washington

- Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.
- Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system
- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation
- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

# State of Washington

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

## **Taxes Receivable (Net of Allowance) - ATLAS**

### **Key Controls #1 as follows for the ATLAS:**

- **Key Control #1 – Automated Interface – Completeness/Valuation** - ATLAS will automatically create a receivable including penalties and interest based on the due date, which is automatically posted by ATLAS in the taxpayer account. If a tax return was not filed by the due date, the day after the due date ATLAS will automatically create an estimated tax return based on the account's reporting history and tax rates.

### **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **STEP 2: Confirm and Test Automated Key Control:**

We met with Ayano Faasumalie, Revenue and Financial Reporting Coordinator, on June 20th, 2024 via TEAMS to discuss the process of ATLAS automatically creating a receivable for submitted returns and estimated returns.

### **Return Receivable**

We performed a walk through of an account in ATLAS with a submitted return with Ayano. She pulled up the tax return for taxpayer UBI No. 604-916-389, a quarterly filer, for the period of 7/1/2023-9/30/2023. The return was due 10/31/2023, however the taxpayer did not file until 11/3/2023 and has not yet paid, as of the date of this walkthrough. Based on information submitted in the return, ATLAS calculated the following taxes:

- Business & Occupation Tax - 195.38 (gross amount \$40,366.79 and a tax rate of 0.00484)
- Small business tax credit - 135.00

This resulted in a total tax balance of \$60.38. However, because the filer was late, ATLAS automatically calculated a penalty of \$20.53 and interest of \$2.02, bringing the total due to \$82.93.

We verified the tax rates used to calculate the above taxes using the DOR website:

- [Business & occupation tax classifications | Washington Department of Revenue](#)

# State of Washington

We determined the total amount of taxes due were correctly calculated.

Ayano showed us the receivable was posted in November in ATLAS for the balance due of \$82.93. The receivable was posted in the Receivable Accumulation General Ledger (GL) in ATLAS by revenue source until month end. If a payment or adjustment is made on the return, it will be subtracted out of the Accumulated Receivable GL. At the end of the month, the balance in the Accumulation GL is moved into the Receivables GL automatically by ATLAS. ***No issues noted.***

## **STEP 3: Understand General IT Controls**

We met with Lucas Kenall and Pavath Phommachanh on May 23, 2024 to gain an understanding of general IT controls over the creation of receivables and the calculating of interest and penalties.

Because calculations for receivables follow the same general IT controls as the calculations for local taxes. We gained our understanding of general IT controls in the Tax Collections for Other Governments section: [Key Control 2 (Automated)].

## **STEP 4: Confirm Key General IT Controls**

We confirmed our key general IT controls in the Tax Collections for Other Governments section: [Key Control 2 (Automated)].

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **D.1.PRG - Taxes Receivables (Net of Allowance)**

*Procedure Step:* Key Control #2 (Automated)

*Prepared By:* BFW, 6/26/2024

*Reviewed By:* RKM, 8/20/2024

Purpose/Conclusion:
---------------------

### **Purpose:**

To determine whether on the last business day of the month, ATLAS automatically prepares and posts Journal Vouchers (JV) by revenue source and receivable type to record the taxes receivable, accrued revenue, unavailable revenue, and the allowance for uncollectibles **(Key Control 2**

## State of Washington

for **ATLAS**) was in place in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - ATLAS\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

- Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

- What formulas are used to make the calculation?
- What values or factors are used to make the calculation? For example:
  - Rate tables used by the calculation
  - Profile fields (i.e., applicable transaction types)
  - Programmed/set formulas and/or values
  - Constraints (i.e., effective date, minimums/maximums, etc.)
- How is the calculation triggered or initiated?
- How is the calculation recorded in the accounting system (or used in an end result)?

#### **Automated Interfaces:**

## State of Washington

- Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?
- What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

- Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

- Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

- Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?
  - What transactions, data, tasks, or documents are approved?
  - Who are the preparers? How do preparers submit for approval?
  - Who are the authorized approvers? Are there backup approvers?
  - What documents or information are required to make approval judgment?
  - What is the next step once a transaction/data/ task/document is approved or denied?
  - Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?



## State of Washington

- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

- What information or exceptions is the report designed to identify (what is the purpose of the report)?
- How is the report used and by whom?
- For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

- What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

# State of Washington

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

## Electronic Approvals:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?
  - What transactions, data, tasks, or documents are approved?
  - Who are the preparers? How do preparers submit for approval?
  - Who are the authorized approvers? Are there backup approvers?
  - What documents or information are required to make approval judgment?
  - What is the next step once a transaction/data/ task/document is approved or denied?
  - Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?
- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

## Software Calculation:

- Re-perform the calculation for selected transactions.

## State of Washington

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

- If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.  
*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*
- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

- Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

- Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

- Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

## State of Washington

- When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

- Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

- For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.
- Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

- Observe a transaction to see the approval process and verify any key aspects of the process or limits.
- If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### Software Calculation:

## State of Washington

- Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.
- How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

- What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

# State of Washington

## Automated Interfaces:

- Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.
- What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*
- How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

## Edit Checks:

- Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.
- How can the edit check be changed or customized?

## State of Washington

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

- What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

- Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.
- How is the report triggered or initiated?

## State of Washington

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

- Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

- If the report is hardcoded into the system, how are program changes made?
- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

- NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

- How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.
- If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?
- If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*



## State of Washington

- What are the procedures to test that program changes are properly working?
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the **SOC Report Reliance** worksheet in the Store.

# State of Washington

## Automated Interfaces:

- Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.
- Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## Edit Checks:

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance*

# State of Washington

*requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

- [Instructions](#) are located in Team IT Audit's System's Sharepoint page.
- Details of IT Security related issues should NOT be included in any emails or helpdesks.
- Exit, ML and Findings should be separately communicated in an IT Security Results Document.
- Findings will be referenced, but not included in the audit report.
- All IT security-related recommendations must be reviewed by [Team IT Audit](#).
- Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

## State of Washington

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

- Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.
- Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.
- Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

## State of Washington

- Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.
- Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.
- Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.
- Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.
- Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.
- Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.
- Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

- Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.
- Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

# State of Washington

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system
- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation
- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

## Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.:

**Taxes Receivable (Net of Allowance) - ATLAS**

# State of Washington

## **Key Controls #2 as follows for the ATLAS:**

- **Key Control #2 – Automated Interface – Existence** – On the last business day of the month, ATLAS automatically prepares and posts Journal Vouchers (JV) by revenue source and receivable type to record the taxes receivable, accrued revenue, unavailable revenue, and the allowance for uncollectible.

## **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

## **STEP 2: Confirm and Test Automated Key Control:**

We met with Ayano Faasumalie, Revenue and Financial Reporting Coordinator, on June 20, 2024 via TEAMS to discuss the process of ATLAS automatically creating a receivable for balance dues and estimated returns.

On the last business day of the month from the Receivables GL, ATLAS automatically prepares and posts a Journal Voucher (JV) by Revenue Source and Receivable type to record receivables into AFRS. Ayano showed us the month end batch JV #140E4493 created in ATLAS to record the return receivables as of 11/30/2023, in the amount of \$13,253,358.50 and the uncollectible amount of \$798,030.46 based on the deferred revenue. Ayano showed us the reconciliation of the JV created by ATLAS to the amounts expected by Revenue Accounting and the amounts tied without exception. *No issues noted.*

## **STEP 3: Understand General IT Controls**

On May 23, 2024 we met with Lucas Kennal, IT APP Development Manager, and Pavath Phommachanh, IT Audit Manager, to gain an understanding of general IT controls relating to the interface between ATLAS and AFRS. Lucas informed us that batches process automatically overnight. ATLAS has a Batch Manager function within the Production Manager tab that is used to track all batches that are processed. Any batch that had an error or failure in processing would be flagged here. Every morning, the Batch Manager is reviewed for files that were flagged with errors or failures and immediately addressed (**General IT Control**). Email verification is also sent out automatically by ATLAS to notify that the transfer was complete and whether errors or failures occurred.

## **STEP 4: Confirm Key General IT Controls**

**Every morning, the Batch Manager is reviewed for files that were flagged with errors or failures and immediately addressed -** Lucas displayed batch file number 2065578 from the previous evening (5/22/2024) with the following details: File Type - FTP (file transfer protocol), Destination - AFRS, Destination File - 62626, Begin - May 22, 2024 21:15:49, End - May 22, 2024 21:15:49, to show us it had been flagged with two items that needed attention. When the file was opened, we could see the two errors had be "cleared out" or remedied by a member of his team already. *No issues noted.*

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed



# State of Washington

at MAX.

## D.1.PRG - Taxes Receivables (Net of Allowance)

*Procedure Step:* Key Control #3 (Manual)

*Prepared By:* BFW, 9/23/2024

*Reviewed By:* RKM, 9/26/2024

Purpose/Conclusion:

### **Purpose:**

To confirm the year-end JV to record June 2024 returns received after June 30, 2024 as a receivable and accrued revenue for FYE, noted in Key Control 3 for ATLAS, in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

## State of Washington

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

## State of Washington

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #3 - Manual - Existence/Completeness** - In August, the ATLAS "gross receipts" report, which is programmed to pull all gross receipts for the period July 1-August 15, is downloaded to Excel and compared to the gross receipts from the prior five years to check that the values seem reasonable. Revenue Accounting will reconcile and review the year end JV to enter into AFRS to show the June returns received after June 30<sup>th</sup> as a receivable and accrued revenue for the FYE.

The understanding for this system is documented above in the "Controls - ATLAS" step.

# State of Washington

## **1. Confirmation of Key Manual Control:**

We confirmed the key control as part of our understanding of retail sales and use taxes and B&O. See confirmation at [[Key Control # 3 \(Manual\)](#)]. ***No issues noted.***

### **Noted Weaknesses are as follows:**

- None.

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.1.PRG - Taxes Receivables (Net of Allowance)**

*Procedure Step:* Key Control #4 (Manual)

*Prepared By:* BFW, 5/21/2024

*Reviewed By:* RKM, 7/4/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To confirm monthly reconciliation between ATLAS and AFRS (key control 4 for ATLAS) in order to assess control risk.

### **Conclusion:**

- We noted **no** material weaknesses or significant deficiencies in internal controls.

## State of Washington

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control #4 - Manual - Existence/Completeness for ATLAS** - At the end of each month, Revenue accounting runs a monthly revenue activity report (MRA) from ATLAS and AFRS revenue report from Enterprise Reporting System. A reconciliation is then performed between ATLAS and AFRS to ensure the reported revenue and receivables amounts are accurate and complete.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

We confirmed this control as part of our review of controls related to retail sales and use taxes and B&O taxes at [[Key Control # 4 \(Manual\)](#)]. *No issues noted.*

### **Noted Weaknesses are as follows:**

- None

### **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.1.PRG - Taxes Receivables (Net of Allowance)**

## State of Washington

*Procedure Step:* Key Control #5 (Manual)  
*Prepared By:* BFW, 6/25/2024  
*Reviewed By:* RKM, 8/5/2024

### Purpose/Conclusion:

#### **Purpose:**

To confirm Revenue Accounting pulls the monthly ATLAS report into a spreadsheet and compares prior months reviewing for anomalies (key control 5 for ATLAS) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude*



## State of Washington

*and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements.*

## State of Washington

*In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #5 - Manual - Existence/Valuation** - Financial Reporting & Systems Support pulls monthly ATLAS report (by receivable type) into a spreadsheet and compares prior months (in same FY) reviewing for anomalies in the receivables and allowance calculations.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

We met with Ayano Faasumalie, Revenue & Financial Reporting Coordinator in Business & Financial Services, on April 24th, 2023 to discuss the receivable type monthly comparison related to allowance for uncollectible accounts. She walked us through the process for running the ATLAS report showing monthly JV excise tax receivables by GL amounts by receivable type (returns, estimated returns, audit, and lien receivables). From the ATLAS transaction tab in the ledger, she is able to export the data in an excel spreadsheet that Allison Walker (one of her staff) uses to compare monthly balances.

## State of Washington

We reviewed the month to month comparison from Ayano on 6/24/2024. The workbook was titled "Fiscal Year 2024 Excise Taxes Receivables". It contained the four types of receivables:

- Return Receivables
- Estimated Return Receivables
- Audit Receivables
- Lien Receivables

Each receivable type had each month summarized. For each month, the sheet detailed balance, uncollectibles, net, local tax, FY24 estimated collections, and unavailable revenue (deferred inflows of resources). The spreadsheet then calculated the balance of the month to month comparison, then used the balance to calculate the percent change.

### Return Receivables as of May 2024

Balance	Uncollectibles	Net Receivables	Local Tax Portion	FY 24 Estimated Collection Accrued Revenue	Unavailable Revenue	Discounted Balance Month-to-month comparisons	Uncollectibles Month-to-month comparisons	Uncollectible/Discounted Balance
GL 1311/1312	GL 1341/1342	Net Receivables	GL 5152	GL 3205	GL 5192	% Change/ \$ Increase (Decrease) from prior month	% Change/ \$ Increase/(Decrease) from prior month	Uncollectible/Discounted Balance % Change
118,737,190.64	(5,661,852.46)	113,075,338.18	(21,097,263.96)	(56,226,202.41)	(35,751,871.81)	0.3% 388,089.78	6.1% (327,309.78)	-4.8%

Thirteen large anomalies were identified and listed on the bottom of the worksheet. Each anomaly listed the amount, the source, account number (so it can be investigated in ATLAS), and when the source occurred.

1) Large audits issued - ADT LLC, 603-190-246 for \$13M (\$14.7M Tax, \$2M P&I, -\$3.6K audit credit). Exotic Metals, 602-223-975, \$2.5M (\$2.4M tax, \$246K P&I). Also includes audit issued to 604-877-765 Qtr. 4, 2021 – Tax for \$4.9 M and P&I for \$2.1 M. This audit was reversed on 10/27/23.

## State of Washington

Also reduction in deferred audit: 12-year write-off included account # 602-635-596 Qtr. 3, 2009 period for \$3.8 million for an audit in deferred collection

2) Uncollectible write-off was done on 7/11/2023 for a total of \$27,974,550.52. Plus some large liens were issued as well.

604-107-324, lien 38837 for \$1.7M on 7/31/2023. 604-042-280, lien 53784 for \$415k on 7/26/23."

3) Audit for \$4M issued with \$500k for P&I to account # 601-959-741 12/2020 period in September. Audit for \$3.6 M issued to account # 601-246-974 6/2022 period in September 2023.

4) a) Audit Allowance for Uncollectible – Uncollectible rate was updated with SQR 14963 from 0.0426 to 0.0477 in ATLAS to reflect corrections made for calculations errors. The receivable JVs for June 2023 was manually updated in FY 2023 FM 25. This changed the audit allowance for - September from \$78.1 million to \$87.2 million.

4) b) Lien Allowance for Uncollectible - Uncollectible rate was updated with SQR 14963 from 0.1573 to 0.1712 in ATLAS to reflect corrections made for calculations errors. The receivable JVs for June 2023 was manually updated in FY 2023 FM 25. This changed the lien allowance for September from \$442.2 million to \$445.8 million.

5) Audit issued in July 2023 for 604-877-765 Qtr. 4, 2021 – Tax for \$4.9 M and P&I for \$2.1 M was reversed on 10/27/23.

6) Due to the implementation of Managed Payments in ATLAS, we encountered some issues with receivable timing. The big issue is when returns are posted before due date, receivables are posting before the return due date. The large increase in January is because of the quarter returns due that month.

We also noted some strange instances where the timing of receivable reduction is off from when the revenue is posted. It gets reduced properly in the end but because of these timing changes, we are seeing fluctuations in the receivable balance at the end of the month when the JVs are generated.

SQR 16186 is being worked on to correct these issues.

7) Compliance Assessments issued for 604-519-175 for 10/23, 11/23, 12/23, 1/24, 2/24 period in total of \$2.2 million. 604-176-001 for 10/2020 period to 12/31/2023 period for \$325k.

8) \$4.5 M payment applied to an audit on account # 602-996-887 Qtr 4 2016 period. \$2.3 M payment applied to an audit on account # 602-759-741 Qtr 4, 2021. \$1.9 M payment applied to an audit on account # 048-006-501 7/2022 period.

9) Uncollectible write-off on 2/2/24 for the amount of \$24 million.

10) Lien issued to a collection with audit on account # 603-115-427 03/2023 period in February 2024. The total of \$6.4 million in audit receivable (\$3.6 M in tax & 2.8 M in P&I) was transferred to \$7.2 million lien receivable (\$3.6 M in tax & \$3.6 M in P&I).

11) Lien issued to a collection on account # 602-230-841 in March. The collection covers period 1/2019 - 12/31/2019 period with balances of \$7.4 million.

12) Audit issued for \$3.4M (\$2.9M tax, \$579k P&I) for 603-398-768, 12/2022 period. Audit issued for \$3.4M (\$3.4M tax \$543k P&I) for 603-064-508 12/2022 period.

13) Lien 67858 issued Excise Tax 604-519-175 on 4/17/24 for \$2,895,256.82.

14) Large audit adjustment for closing agreement 5766653, excise tax, 178-005-030, 12/31/2018 period. Adjustments for \$21,317,845.89 (Audit tax \$14.5M, P&I \$4M, \$2.7M payment)

# State of Washington

Ayano informed us that all anomalies noted are confirmed as legitimate prior to being noted on the spreadsheet, this is their way of tracking items.  
***No issues noted.***

## **Noted Weaknesses are as follows:**

- None

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **D.1.PRG - Taxes Receivables (Net of Allowance)**

*Procedure Step:* Risk Assessment

*Prepared By:* BFW, 8/1/2024

*Reviewed By:* CJG, 11/21/2024

Purpose/Conclusion.\*

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy.\*

Auditors are **required** to perform the following procedures for each line item:

1. Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance

## State of Washington

or class of transactions.

*Inherent risk is the susceptibility of an assertion to a material misstatement, assuming that there are no related controls. Inherent risk can be thought of as the "threat" of misstatement. Inherent risk exists independently of control risk (the level of threat exists independent of the level of vulnerability to threats). Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*
  - *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*
  - *Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*
  - *Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*
- *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*
  - *Are there substantial pressures or motivations to misstate the balance?*
- *Inherent Risk due to Misappropriation*
  - *Is the account balance or transaction class susceptible to sizable misappropriation?*
- *Inherent Risk due to Non-Compliance*
  - *Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

## State of Washington

- *Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*
- *Are there any motivations or pressures to not comply?*

2. Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and testing (if applicable). If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*In order to set control risk to LOW, general controls would also need to be tested to provide evidence of the consistent operation of automated controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body.*

***All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

- 3. Assess the risk of material misstatement for each relevant assertion for each material line item. The risk of material misstatement is a combination of the auditor's separate assessment of inherent and control risk.

*The Risk of Material Misstatement is a combined assessment of inherent and control risk based on auditor's judgment. If inherent and control risk are assessed differently, it is a matter of professional judgment as to whether the combined assessment is moderate or if one factor outweighs the other.*

4. Design a substantive testing strategy that addresses the relevant assertion in all significant transaction streams included within the material line item.

*In addition to identifying what to audit (material balances) and what to audit for (relevant assertions), planning has also identified how much to audit (risk of material misstatement). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- **Existence - Moderate**
- **Valuation - Moderate**
- **Completeness - Moderate**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

- **ATLAS - Existence, Valuation, and Completeness**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

- **Existence - Moderate**
- **Valuation - Moderate**



# State of Washington

- **Completeness - Moderate**

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

### **Valuation**

- We will recalculate taxes assessed for a sample of registered taxpayers to ensure rates are being applied appropriately and therefore tax revenue and receivables are recorded at proper amounts. We will test these tax rates as part of the tax revenue testing.
- To determine if the allowance for uncollectible accounts for excise taxes was valued at proper amounts, we will use the FYE ATLAS Summary report to determine the deferred receivable balance in ATLAS. We will vouch the deferred balances for all receivable types to the ATLAS GL ledger report for GL 1341 and 1348 and compare the balances to amounts recorded in AFRS. We will compare the FY24 balance for allowance for uncollectible to the prior two years to determine if the amount for FY24 appears reasonable, including comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

### **Existence/Valuation/Completeness**

- We will test a sample of sales, use, and business and occupation taxes receivable recorded in ATLAS at FYE to ensure they exist and the value is properly supported by verifying the transactions match corresponding tax returns and were included in an accumulation GL within ATLAS. We will trace the GL amount to a batch posted in AFRS. Additionally, we will verify each batch ties to AFRS.
- We will select a sample of sales, use, and business & occupation accrual transactions from the gross receipts accrual JV and verify that the transactions were recorded for the correct amount and in the proper period. We will test the accrual JV as part of the tax revenue testing.
- We will review the A8 from each county for each of the months selected by the JV selection process during deferred inflows. We will ensure the total remitted to OST by all the counties matched the total remitted by OST to DOR.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **D.1.PRG - Taxes Receivables (Net of Allowance)**

*Procedure Step:* Substantive Test

*Prepared By:* BFW, 10/3/2024

*Reviewed By:* SHW, 11/6/2024

# State of Washington

## Purpose/Conclusion:

### **Purpose:**

To determine whether:

Reported receivables represent amounts uncollected as of the end of the period (Existence).

Receivables were reported at properly valued or calculated amounts (Valuation).

All receivables were reported as of the end of the period (Completeness).

### **Conclusion:**

We determined that reported receivables represent amounts uncollected as of the end of the period (Existence); receivables were reported at properly valued or calculated amounts (Valuation); and that all receivables were reported as of the end of the period (Completeness). **No issues noted.**

## Testing Strategy:

### **Existence:**

The following is a list of **considerations** for testing the existence assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Receivables**

- Confirm receivables with the obligated party.
- Confirm intergovernmental receivables with the other agency.
- Confirm trade receivables using negative or positive confirmations to customers. *NOTE: if trade receivables were not confirmed, auditors should document the reasons for not following the audit requirement (see policy/criteria tab).*
- Verify receivables to source billing documents, reimbursement requests or other documentation.
- If receivables are sent to an external collection agency or trigger an action that affects the obligated party (ie: water shut-off) within a reasonably short time period, trace or reconcile from the A/R Aging report to the collection agency's report or evidence of a confirming action.
- Verify receivables through subsequent receipt of funds (remittance documentation should evidence the period to which it applies).
- For the period following balance sheet date, scan the accounts receivable general ledger control account for material charge-off and unusual transactions, and investigate.

## State of Washington

Perform analytical procedures to determine the reasonableness of receivable balances and follow-up on any unexpected results. For example, trend analysis of aged A/R, trend of beginning balance, billings, adjustments, payments and ending balance, inventory/volume usage reconciliation, etc.

### Valuation:

The following is a list of **considerations** for testing the valuation assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

- Review the entity's calculation of the value of intangible assets.
- Review the entity's calculation of write-off of inventory or other assets due to obsolescence or damage.

### **Calculation or Realizable Value of Receivables**

- Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.
- Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.
- Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### Completeness:

The following is a list of **considerations** for testing the completeness assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Receivables**

- Inquire regarding whether amounts earned but not yet received as of year-end were accrued. Consider follow-up review of documentation to verify inquiry.
- Consider entity activities and follow-up on activities where receivables would be expected, but none are recorded.
- Verify that interest and penalties are being billed to delinquent accounts in accordance with entity policy.

Guidance/Criteria:

Record of Work Done:

# State of Washington

## **Taxes Receivable Testing Coverage**

To ensure testing provided a sufficient amount of coverage of the taxes receivable balance, we received a breakdown of the taxes receivable balance from Ayano Faasumalie, Revenue & Financial Reporting Coordinator, and reconciled the breakdown to ACFR balances included in the lead sheet at [\[Line Item Lead Sheet\]](#). We determined the breakdown was representative of the ACFR balance. We identified the following taxes as the most significant:

- Property Tax - 31.40%
- Gross Receipts - 38.39%
- Sales, Use, and B&O Taxes Receivable - 20.46%

We noted procedures performed as part of our deferred inflows of resources testing at [\[Property Tax Collection Testing\]](#) provided sufficient coverage of property tax receivable and procedures performed as part of our retail sales and use and B&O tax revenues testing at [\[Accrual JV Testing\]](#) provided sufficient coverage over the gross receipts portion of the balance. We tested a sample of sales, use, and business and occupation taxes receivable recorded in ATLAS at FYE to ensure they exist and the value is properly supported by verifying the transactions match corresponding tax returns and were included in an accumulation GL within ATLAS. We traced the GL amount to a batch posted in AFRS. Additionally, we verified each batch ties to AFRS, see testing here: [\[Tax Revenue Testing\]](#). Based on the work performed as part of other steps within the ACFR, we determined testing the Sales, Use, and B&O Taxes Receivable would provide sufficient coverage over the entire taxes receivable balance. In total, the testing procedures noted above cover 90% of the taxes receivable balance. See our testing summary and lead sheet reconciliation at [\[Taxes Receivable Testing\]](#) in the tab, "Testing Summary". ***No issues noted.***

We obtained a list of all general fund sales, use, and business and occupation (B&O) taxes receivable from ATLAS as of June 30, 2024 from Ayano Faasumalie, Revenue & Financial Reporting Coordinator in Business and Financial Services. The testing population is all of the receivable transactions that make up the FYE 2024 taxes receivable JV pulled from ATLAS. We reconciled the testing population to AFRS entries as part of the spreadsheet at [\[Taxes Receivable Testing\]](#), see tab "Testing Summary". We determined the population to be complete and used the testing population to select samples for the substantive tests to meet the existence/completeness/valuation assertions below.

## **Substantive tests performed to meet the Existence assertion:**

We haphazardly selected a sample of 30 transactions from the testing population. To ensure existence for the selected transactions we performed the following substantive tests:

- Receivable ties to supporting documentation (tax return or audit working paper) in ATLAS?
- Documentation (Collection Notes) supports deferred status in ATLAS?

For each selection, we reviewed the revenue tab within the taxpayer's account and tied recorded amounts to tax returns for the applicable filing period. For deferred taxpayers, we reviewed collection notes to ensure the taxpayer's deferred status was supported to be uncollectible. We determined selected transactions existed in the current audit period. ***No issues noted.*** See testing performed at [\[Taxes Receivable Testing\]](#) in the "FS Substantive Sample" tab.

## State of Washington

### **Substantive tests performed to meet the Completeness assertion:**

Using the above mentioned haphazardly selected sample of 30 transactions, to ensure completeness for the selected transactions, we performed the following substantive tests:

- Receivable processed in receivable accumulation in ATLAS?
- Receivable included in June 30, 2024 month end batch receivable recorded in AFRS?

For each selection, we reviewed the revenue tab within the taxpayer's account and the history sub tab which was navigated to the revenue account spring board page. Within ATLAS, a hyper link for the ATLAS receivable accumulation that the transaction was included could be followed from there. We traced each taxpayer account to the ATLAS accumulation and further traced the ATLAS accumulation to the year end entry to AFRS using additional hyperlinks to ensure transactions were included as receivables. For selected taxpayers in deferred status, we reviewed the transaction type posted in the year end receivables JV to ensure amounts were properly included as allowance for uncollectible accounts. We determined taxes receivable were complete. ***No issues noted.*** See testing performed at [[Taxes Receivable Testing](#)] in the "FS Substantive Sample" tab.

### **Substantive tests performed to meet the Valuation assertion:**

Using the above mentioned haphazardly selected sample of 30 transactions, to ensure accurate valuation for the selected transactions, we performed the following substantive tests:

- Receivable ties to supporting documentation (tax return or audit working paper) in ATLAS?
- Receivable processed in GL accumulation in ATLAS?
- Documentation (collection notes) supports deferred status in ATLAS?

For each selection, we reviewed the revenue tab within the taxpayer's account and tied recorded amounts to tax returns/audit working paper. We ensured deferred status taxpayers were supported by collection notes and traced all selected transactions to the ATLAS accumulation GL and AFRS year end entry to ensure deferred accounts were recorded as uncollectible and the other receivable types were accurately valued within AFRS based on support. We determined receivables were properly valued. ***No issues noted.*** See testing performed at [[Taxes Receivable Testing](#)] in the "FS Substantive Sample" tab.

### **Allowance for Uncollectible Testing:** [[Allowance for Uncollectible](#)]

We also performed a review of the allowance for uncollectible accounts related to fund 001 - Excise Taxes. We obtained the ATLAS summary report of all receivable types at FYE 2024 and tied the amounts to year end entries within AFRS from Webi to ensure amounts were properly valued for the ACFR. We noted immaterial differences for GL 1341 (Allowance for Uncollectible Account for Return, estimated, audit receivable type) between AFRS and the ATLAS summary ledger report. We compared the FY24 balance for allowance for uncollectible to the prior two years and determined the amount for FY24 appears reasonable, based on expectations, including comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables. We determined allowance for uncollectible amounts were properly valued. ***No issues noted.***

# State of Washington

## D.2.PRG - Retail Sales and Use and B&O Taxes

*Procedure Step:* Summary & Conclusion

*Prepared By:* BFW, 10/15/2024

*Reviewed By:* CJG, 11/21/2024

Purpose/Conclusion:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

## State of Washington

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the **Permanent File** folder or assessment of control risk?
  - If circumvention, the **Management Override of Controls** step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate

## State of Washington

evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done.:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **D.2.PRG - Retail Sales and Use and B&O Taxes**

*Procedure Step:* Understanding of Line Item

*Prepared By:* BFW, 5/16/2024

*Reviewed By:* RKM, 5/29/2024

Purpose/Conclusion.:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.



# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associated with the line item.
- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

## State of Washington

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions:**

There were no prior year audit exceptions for this balance.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)]

The Department of Revenue collects and administers a majority of Washington's General Fund-State (GF-S) revenue, accounting for 95% of the total GF-S revenue forecasted for 2023-25 biennium in February 2024. Some of the largest tax sources include:

- Retail sales and use tax
- Business and occupation tax
- Property tax

The state closely monitors DOR revenues, which are significant to the state's budgeting and spending decisions. Because these revenues are connected with business activities (sales and business revenues), the balances for Sales tax, Use Tax and Business & Occupation Tax fluctuate with how the economy in general is doing. The Economic and Revenue Forecast Council provide forecasts of the State's revenues [[Publications | Washington State Economic and Revenue Forecast Council](#)], factoring in known changes in the economy, see the February 2024 quarterly forecast at [ERFC February 2024](#).

Based on prior ACFR audit work, we determined the Forecast Council is fairly accurate at projecting Retail Sales and Business and Occupation tax receipts. The February 2024 quarterly report summarizes that GF-S revenue collections since the November 2023 forecast are \$70.8 million (0.9%) above the forecasted amount. The forecasted increase for the rest of the 2023-25 biennium is \$121.8 million.

# State of Washington

## **Retail Sales and Use Taxes**

Retail sales and use taxes (collectively referred to as retail sales tax) is the largest source of general fund revenue and accounted for approximately 51% of general fund revenues in FY23, excluding Federal Grants-in-Aid. The state's share of retail sales tax is 6.5% of the sales prices. Counties and local jurisdictions impose sales tax percentages on top of the retail sales tax. See our understanding of collections and payments of local tax for other governments at [\[Summary & Conclusion\]](#) and [\[Controls - ATLAS\]](#). Retail sales tax revenue increased from \$14.90 billion in FY22 to \$15.81 billion in FY23 and is projected to be \$15.92 billion in FY24 (per Forecast Council projections, see ERFC table 3.9 - GF-S forecast detail at [ERFC February 2024](#)). The revenue source code for retail sales tax is 101/102 and for use tax 110/111.

## **Business and Occupation Taxes**

The Business and Occupation Tax is the second largest source of non-exchange revenue for the general fund and accounted for approximately 20% of general fund revenues in FY23, excluding Federal Grants-in-Aid. This line item balance is made up of business and occupation tax (Source Code 105) and business and occupation tax credits (Source Code 106), which is tax on the gross receipts of all businesses operating in Washington. Business and occupation tax revenue increased from \$5.67 billion in FY22 to \$6.23 billion in FY23 and is further projected to increase to be \$6.39 billion in FY24 (Per Forecast Council projections, see ERFC table 3.9 - GF-S forecast detail at [ERFC February 2024](#)).

### **Change Analysis:**

We obtained the Internal Audit risk assessment for revenues and receivables for FY2023 from Sandi Fairchild, Chief Financial Officer, and inquired with Ayano Faasumalie, Revenue & Financial Reporting Coordinator, and noted no significant changes to retail sales and use and B&O Taxes.

### **(3) Updates to Significant Account Matrix:**

We identified no changes that need to be made to the Significant Account Matrix.

## **D.2.PRG - Retail Sales and Use and B&O Taxes**

*Procedure Step:* Controls - ATLAS

*Prepared By:* BFW, 5/16/2024

*Reviewed By:* RKM, 10/11/2024

Purpose/Conclusion:

### **Purpose:**

# State of Washington

To gain an understanding of internal controls.

## **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

## **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

## State of Washington

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

# State of Washington

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

- Internal controls in the Automated Tax and Licensing Administration System (ATLAS) address the following balance(s):
  - **Taxes, net of available credits: Sales and Use** - Governmental Activities
  - **Retail sales and use taxes** - General Fund
  - **Taxes, net of available credits: Business and Occupation** - Governmental Activities
  - **Business and Occupation Taxes** - General Fund

For the following assertions:

- **Occurrence** - There is a risk of improper revenue recognition resulting in the year-end accrual being overstated. There is a risk that recorded revenue is more than source records.
- **Completeness** - There is a risk that certain revenues are not reported or accrued.
- **Valuation** - There is a risk that tax revenues are incorrectly calculated.

## **Background**

In March 2018, DOR implemented the Automated Tax and Licensing Administration System (ATLAS), which replaced all other systems and streamlined the process for recording tax return payments received into AFRS. Electronic filing (E-file) is the preferred method for tax return filing and the majority of taxpayers are required to file electronically. The payment methods available to taxpayers did not change with the implementation of ATLAS and the payment methods are EFT, E-check, Credit Card, and physical check.

## **Gain an Understanding of Internal Controls**

# State of Washington

We met with Ayano Faasumalie, Revenue & Financial Reporting Coordinator, on April 10, 2024 to gain an understanding of controls over retail sales and use and B&O taxes.

## **Tax Returns**

The majority of tax returns are received electronically and filed through the online taxpayer system, My DOR, which is part of the State's Secure Access Washington (SAW) application created by the Washington Technology Solutions (WaTech). Returns filed in My DOR are sent directly into ATLAS, which is coded to automatically calculate taxes due based on the information entered by the taxpayer on the return.

When a taxpayer logs into their My DOR account and selects to file a return, ATLAS automatically calculates taxes due from pre-programmed rates based on return information entered by the taxpayer (**Key Control #1- Automated- Valuation**). When the taxpayer submits the return, taxes due and the payment amount are recorded in the transactions tab of ATLAS. Additionally, information such as the date filed, the date paid, and any changes or adjustments made to the return or the taxpayer's account will also be recorded in the transactions tab of ATLAS. My DOR and ATLAS only allow a return to be filed once and ATLAS will create a work item for duplicate return received if the taxpayer attempts to submit a paper return for the same return period received. Logic checks are run when the return is processed. If there is an error, the return is flagged and sent to a work queue for an Examiner to review. Returns flagged for review do not get recorded to the appropriate revenue source until errors are resolved and released from the queue.

## **How transactions are recorded in AFRS:**

### **Cash Journal Entries**

When payments are received via ACH/debit, ACH/credit, wire transfer, and cash/check from field offices, ATLAS automatically generates an A8 cash journal (CJ) to record the cash receipts. For payments received by credit card, lockbox and via mail/FedEx/UPS, a manual CJ is created in ATLAS by Treasury Management in Business & Financial Services (B&FS). Treasury Management staff batch the documents and prepare the deposits assuring they both balance. Once they are entered, the Batch Control System (BCS) compares the total of the individual batches to what was deposited for the day. The A8s are sent to the State Treasurer's Office (OST) for deposit entry into the Treasury Management System and verification that all funds have been received. If the payment amount received by the OST does not match DOR's A8, they will contact DOR and inform them of the out of balance condition. Treasury Management will follow up on the difference by totaling and comparing the documents and payments. The Batch Sheet which contains the batch amount totals, document count, batch date, and batch number is placed on top, and the batch is forwarded to Taxpayer Account Administration (TAA). Treasury Management then reconciles the ATLAS cash journal report totals to the total deposit recorded in the OST's concentration account to ensure they match.

DOR's Revenue Accounting section in B&FS verifies the CJ batches are error free and releases for processing in AFRS at the end of each day. ATLAS initially records the deposit in Fund 01P (Suspense Account) and then distributes from suspense to the proper revenue source codes once the returns and payments are applied to the taxpayers' accounts. If the payment is identified as Excise Tax but not applied to a tax return, the fund is transferred to the general fund Revenue Act revenue source (01-99 – Tax Revenue Suspense). If tax payments are not applied to the taxpayer's account due to mismatched returns or errors that need to be resolved, the funds will remain in the suspense account until issues are

## State of Washington

resolved by Tax Examiners. Once the payment has been applied to the taxpayer's account, ATLAS will automatically create a journal voucher to move the funds to the appropriate revenue sources (**Key Control #2- Automated- Valuation/Occurrence/Completeness**). Batches are created and transmitted to AFRS in the evening. Revenue Accounting reviews the batch the following day and releases them in AFRS.

One business day after the tax return is due, ATLAS will automatically create a receivable on the taxpayer's account if there is a balance due (no payment or partial payment with a return). If no return has been filed, one week after the due date, ATLAS will automatically estimate the tax amount due based on historical information in the taxpayer's account. Compliance is responsible for collecting the receivables from all revenue sources, which account for a majority of the agency's debt. DOR does not use an external collection agency to aid in the collection process. The Compliance staff does not receipt any payments on the delinquent accounts. Electronic delinquency notices are sent automatically to taxpayers. For monthly and quarterly filers, DOR sends the electronic notice 10 days from the return's statutory due date. For annual filers, DOR sends them 20 days from the return's statutory due date. We gained an understanding of taxes receivable at [[Controls - ATLAS](#)].

### Gross Receipts Accrual Entry

For monthly filers, excise tax returns for June activity are due July 25th and for quarterly filers, tax returns for the 4th fiscal quarter (April, May, and June) are due July 31st. In August, the ATLAS "gross receipts" report, which is programmed to pull all gross receipts for the period July 1 - August 15, is downloaded to Excel and compared to the gross receipts from the prior five years to check that the values seem reasonable. Revenue Accounting will prepare a JV to enter into AFRS to show the June returns received after June 30<sup>th</sup> as a receivable and accrued revenue for the FYE.

We met with Jerry Tilson, Revenue Accounting Manager, on April 10, 2024 to discuss the gross receipts accrual entry. Jerry explained that towards the end of August, he runs the "gross receipts" report from ATLAS for receipts received between July 1 - August 15 for the tax filing period of June 30 and exports the data to Excel. Once the data is exported into Excel, he sorts by fund and revenue source. The data is then automatically pulled into the "taxpayer assessed taxes (tat) worksheet" tab where the gross receipts are summarized by tax type. Jerry then reviews the report for any errors or major changes and compares the amounts to the prior 5 years for reasonableness. Any significant changes are noted and documented at the bottom of the taxpayer assessed taxes report. After reviewing the report, Jerry verifies that the total gross receipts amount on the "taxpayer assessed taxes report" tab matches the total on the "combined gross receipts adj" tab to ensure that the data from the gross receipts report was pulled in correctly. The JV is then created by pulling the data from the "taxpayer assessed taxes report" tab and input into AFRS by a Revenue Accounting Fiscal Analyst and reviewed and released by Jerry. Additionally, Binh Vu, Accounting Manager, reviews all fiscal-year end JVs. A fiscal analyst reviews the AFRS daily transaction report the next business day to ensure that the accruals were recorded in AFRS accurately and occurred in the correct period (**Key Control #3 - Manual - Valuation/Occurrence/Completeness**).

### Reconciliation Process

ATLAS receives a daily reconciliation file from AFRS and performs an automatic reconciliation between the data recorded in AFRS and ATLAS to ensure revenues recorded are accurate and complete. OFM sends an AFRS download into a SFT folder daily that is picked up by ATLAS. ATLAS then automatically performs a reconciliation between the journal voucher batches in ATLAS from the prior day to the revenues recorded in AFRS.



## State of Washington

Once the reconciliation is complete, ATLAS will update the batch with the reconciliation date under the "reconciled" column. There have been a few issues where the AFRS file was not received and some batches did not go through the automatic reconciliation. Revenue Accounting reviews each batch in ATLAS for a "reconciliation date" to ensure the reconciliation took place. If the AFRS file is not received, Revenue Accounting will contact OFM for the file. However, if the request is made 10 days or more after the date the batches were processed in AFRS, the AFRS data is no longer available for transmission. If the batch does not go through the automatic reconciliation, Revenue Accounting will perform a manual reconciliation.

At the beginning of the month, Jerry Tilson, Revenue Accounting Manager, runs the Revenue GL Monthly Revenue Activity report (MRA) from ATLAS for the previous month. Jerry prints the report from ATLAS and then inputs all of the data into the Monthly Revenue Activity spreadsheet. A reconciliation is then performed between ATLAS and AFRS to ensure the reported amounts are accurate and complete (**Key Control #4 - Manual - Occurrence/Completeness**). Jerry uses a Webi report that runs data based on funds and sources that are applicable to DOR and allows him to link the report directly to the monthly revenue activity spreadsheet. The monthly receivables in ATLAS are reversed out on the Accrued Revenue tab and the new monthly receivable amounts are entered. The receivables are included as part of the monthly activity and netted against cash revenues in the reconciliation of the balance. Jerry maintains a Monthly Revenue Activity spreadsheet to reconcile ATLAS and AFRS using reports from ATLAS and Webi. The spreadsheet is broken down by GL and split into the following tabs:

- **CASH** - Includes GL 4310
- **CASH REVENUE** - Includes GL 3210
- **ACCRUED REVENUE** - Includes GL 3205

Within each tab, the GL data is separated by fund/revenue source. Totals from each tab for the fund/source links to the "Balance" tab on the spreadsheet under the "spreadsheet monthly activity" column. The Webi report is linked directly to the "Balance" tab of the spreadsheet under the "AFRS monthly activity" column.

Once all of the data from both reports has been input into the spreadsheet, Jerry scrolls through the "Balance" tab and checks for any differences between ATLAS and AFRS in the "difference" column. If there is a difference between ATLAS and AFRS, Jerry will highlight the number to be reviewed and researched to determine why there is a difference. In addition to checking for differences for the month, Jerry also compares biennium-to-date balances for ATLAS and AFRS to help check for formula or data errors in the monthly data. Once Jerry has completed the reconciliation and researched any discrepancies or differences, he e-mails relevant parties, including the Economic and Revenue Forecast Council and the Research and Fiscal Analysis Division of DOR, to let them know the report is complete and saved on the J Drive for their forecasts and analysis. In this report, only "Cash", "Accrued revenue", and "Local dist" tabs are viewable. The rest of the back-up tabs are hidden.

### **Key controls are as follows:**

**Key Control #1 - (Automated) - Valuation** - When a taxpayer logs into their My DOR account and selects to file a return, ATLAS automatically calculates taxes due from pre-programmed rates based on return information entered by the taxpayer.

## State of Washington

**Key Control #2 - (Automated) - Valuation/Occurrence/Completeness** - Once the payment has been applied to the taxpayer's account, ATLAS will automatically create a journal voucher to record the funds to the appropriate revenue source. Batches are created and transmitted to AFRS in the evening. Revenue Accounting releases and reviews the batch in AFRS the following day to ensure amounts applied are accurate, complete and assigned to the proper revenue source.

**Key Control #3 - (Manual) - Valuation/Occurrence/Completeness** - In August, the ATLAS "gross receipts" report, which is programmed to pull all gross receipts for the period July 1-August 15, is downloaded to Excel and compared to the gross receipts from the prior five years to check that the values seem reasonable. Revenue Accounting will reconcile and review the year end JV to enter into AFRS to show the June returns received after June 30<sup>th</sup> as a receivable and accrued revenue for the FYE.

**Key Control #4 - (Manual) - Occurrence/Completeness** - At the end of each month, Revenue Accounting runs a monthly revenue activity report (MRA) from ATLAS and AFRS revenue report from Enterprise Reporting System. A reconciliation is then performed between ATLAS and AFRS to ensure the reported amounts are accurate and complete.

**Noted Weaknesses are as follows:**

- None

### D.2.PRG - Retail Sales and Use and B&O Taxes

*Procedure Step:* Key Control #1 (Automated)

*Prepared By:* BFW, 9/30/2024

*Reviewed By:* RKM, 10/11/2024

Purpose/Conclusion.*
----------------------

**Purpose:**

To determine whether ATLAS calculates the taxes due based on information entered by the taxpayer (Key Control 1 for ATLAS) was in place in order to assess control risk.

**Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

# State of Washington

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

- Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

- What formulas are used to make the calculation?
- What values or factors are used to make the calculation? For example:
  - Rate tables used by the calculation
  - Profile fields (i.e., applicable transaction types)
  - Programmed/set formulas and/or values
  - Constraints (i.e., effective date, minimums/maximums, etc.)
- How is the calculation triggered or initiated?
- How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

- Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?
- What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

## State of Washington

- Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

- Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

- Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?
  - What transactions, data, tasks, or documents are approved?
  - Who are the preparers? How do preparers submit for approval?
  - Who are the authorized approvers? Are there backup approvers?
  - What documents or information are required to make approval judgment?
  - What is the next step once a transaction/data/ task/document is approved or denied?
  - Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?
- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

## State of Washington

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

- What information or exceptions is the report designed to identify (what is the purpose of the report)?
- How is the report used and by whom?
- For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

- What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?

## State of Washington

- What transactions, data, tasks, or documents are approved?
- Who are the preparers? How do preparers submit for approval?
- Who are the authorized approvers? Are there backup approvers?
- What documents or information are required to make approval judgment?
- What is the next step once a transaction/data/ task/document is approved or denied?
- Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?
- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

- Re-perform the calculation for selected transactions.  
*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

## State of Washington

- If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.  
*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*
- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

- Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

- Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

- Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.
- When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

- Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each*

## State of Washington

*significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

- For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.
- Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

- Observe a transaction to see the approval process and verify any key aspects of the process or limits.
- If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### Software Calculation:

- Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.
- How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the*



## State of Washington

*changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

- What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

- Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.
- What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for*

## State of Washington

*requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*
- How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

- Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.
- How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

- What are the procedures to authorize and make program changes or configuration/setting changes?

## State of Washington

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

- Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.
- How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

- Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception*

## State of Washington

*report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

- If the report is hardcoded into the system, how are program changes made?
- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

- NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

- How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.
- If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?
- If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

## State of Washington

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the **SOC Report Reliance** workpaper in the Store.

#### **Automated Interfaces:**

- Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.
- Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

## State of Washington

- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

- [Instructions](#) are located in Team IT Audit's System's Sharepoint page.

## State of Washington

- Details of IT Security related issues should NOT be included in any emails or helpdesks.
- Exit, ML and Findings should be separately communicated in an IT Security Results Document.
- Findings will be referenced, but not included in the audit report.
- All IT security-related recommendations must be reviewed by [Team IT Audit](#).
- Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

### **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.



## State of Washington

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

- Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.
- Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.
- Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).
- Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.
- Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.
- Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

## State of Washington

- Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.
- Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.
- Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.
- Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

- Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.
- Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

## State of Washington

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system
- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation
- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.
----------------------

**Key Control #1 - (Automated) - Valuation** When a taxpayer logs into their myDOR account and selects to file a return, ATLAS automatically calculates taxes due from pre-programmed rates based on return information entered by the taxpayer.

### **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

# State of Washington

## **STEP 2: Confirm and Test Automated Key Control:**

To confirm the automated control, we re-performed the tax calculations for a sample of tax returns at [[Tax Revenue Testing](#)]. See "IT Control Testing - Valuation" tab.

## **STEP 3: Understand General IT Controls**

We gained an understanding of general controls in the Tax Collections for Other Governments section, as the processes are identical regardless of the type of tax being calculated, see here: [[Key Control 2 \(Automated\)](#)].

## **STEP 4: Confirm Key General IT Controls**

We confirmed general IT controls in the Tax Collections for Other Governments section, as the processes are identical regardless of the type of tax being calculated, see here: [[Key Control 2 \(Automated\)](#)].

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **D.2.PRG - Retail Sales and Use and B&O Taxes**

*Procedure Step:* Key Control #2 (Automated)

*Prepared By:* BFW, 9/24/2024

*Reviewed By:* RKM, 9/30/2024

Purpose/Conclusion:
---------------------

### **Purpose:**

To determine whether ATLAS will automatically create a journal voucher to record the funds to the appropriate revenue source. Batches are created and transmitted to AFRS in the evening. Revenue Accounting releases and reviews the batch in AFRS the following day to ensure amounts applied are accurate, complete and assigned to the proper revenue source.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently

## State of Washington

during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

- Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

- What formulas are used to make the calculation?
- What values or factors are used to make the calculation? For example:
  - Rate tables used by the calculation
  - Profile fields (i.e., applicable transaction types)
  - Programmed/set formulas and/or values
  - Constraints (i.e., effective date, minimums/maximums, etc.)
- How is the calculation triggered or initiated?
- How is the calculation recorded in the accounting system (or used in an end result)?

#### **Automated Interfaces:**

- Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?
- What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

## State of Washington

- Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

- Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

- Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?
  - What transactions, data, tasks, or documents are approved?
  - Who are the preparers? How do preparers submit for approval?
  - Who are the authorized approvers? Are there backup approvers?
  - What documents or information are required to make approval judgment?
  - What is the next step once a transaction/data/ task/document is approved or denied?
  - Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?
- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

## State of Washington

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

- What information or exceptions is the report designed to identify (what is the purpose of the report)?
- How is the report used and by whom?
- For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

- What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

- Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?
- What is the approval process in the application?
  - What transactions, data, tasks, or documents are approved?

## State of Washington

- Who are the preparers? How do preparers submit for approval?
- Who are the authorized approvers? Are there backup approvers?
- What documents or information are required to make approval judgment?
- What is the next step once a transaction/data/ task/document is approved or denied?
- Is there any exception situations where approval can be by-passed or waived?
- Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?
- Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?
- Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

- Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

- Re-perform the calculation for selected transactions.  
*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*



## State of Washington

- If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.  
*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*
- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

- Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

- Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

- Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.
- When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

- Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each*

## State of Washington

*significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

- For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.
- Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

- Observe a transaction to see the approval process and verify any key aspects of the process or limits.
- If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### Software Calculation:

- Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.
- How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the*

## State of Washington

*changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

- What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

- Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.
- What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for*

## State of Washington

*requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*
- How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

- Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.
- How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

- What are the procedures to authorize and make program changes or configuration/setting changes?

## State of Washington

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?  
*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

- Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.
- How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

- Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception*

## State of Washington

*report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

- If the report is hardcoded into the system, how are program changes made?
- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

- NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

- How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.
- If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?
- If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

- What are the procedures to test that program changes are properly working?
- How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

## State of Washington

- If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the **SOC Report Reliance** workpaper in the Store.

#### **Automated Interfaces:**

- Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.
- Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

- If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.



## State of Washington

- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

- [Instructions](#) are located in Team IT Audit's System's Sharepoint page.

## State of Washington

- Details of IT Security related issues should NOT be included in any emails or helpdesks.
- Exit, ML and Findings should be separately communicated in an IT Security Results Document.
- Findings will be referenced, but not included in the audit report.
- All IT security-related recommendations must be reviewed by [Team IT Audit](#).
- Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

### **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

## State of Washington

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

- Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.
- Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.
- Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).
- Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.
- Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.
- Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

## State of Washington

- Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.
- Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.
- Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.
- Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

- Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.
- Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

## State of Washington

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system
- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation
- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.:
-----------------------

**Key Control #2 - (Automated) - Valuation/Occurrence/Completeness** - Once the payment has been applied to the taxpayer’s account, ATLAS will automatically create a journal voucher to record the funds to the appropriate revenue source. Batches are created and transmitted to AFRS in the evening. Revenue Accounting releases and reviews the batch in AFRS the following day to ensure amounts applied are accurate, complete and assigned to the proper revenue source.

# State of Washington

## **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

## **STEP 2: Confirm and Test Automated Key Control:**

We met with Ayano Faasumalie, Revenue & Financial Reporting Coordinator in Business & Financial Services, on April 16, 2024 via teams to walkthrough the daily JV creation in ATLAS.

We requested Ayano provide the taxpayer account information for North Spokane Women's Health. We noted North Spokane Women's Health filed a monthly tax return for the period of February 2024 on March 25, 2024. Total tax due of \$4,277.37 was made up of the following:

- B&O - \$4,277.37

We performed a recalculation of this account as part of testing at [Tax Revenue Testing] and confirmed rates were applied accurately. We reviewed the history tab for the account within ATLAS and noted the return payment was received on 3/27/2024. The following day, 3/28/2024, the daily JV created by ATLAS was prepared and released. JV #140E1015 with a batch total amount of \$400,473,619.71 was automatically recorded from ATLAS to AFRS. Revenue Accounting reviewed and released the batch on 3/28/2024. ***No issues noted.***

## **STEP 3: Understand General IT Controls**

We gained an understanding of general IT controls as part of the Taxes Receivable (Net of Allowance) section: [Key Control #2 (Automated)].

## **STEP 4: Confirm Key General IT Controls**

We confirmed general IT controls as part of the Taxes Receivable (Net of Allowance) section: [Key Control #2 (Automated)].

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **D.2.PRG - Retail Sales and Use and B&O Taxes**

*Procedure Step:* Key Control # 3 (Manual)

*Prepared By:* BFW, 9/19/2024

*Reviewed By:* RKM, 9/25/2024

## State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm the year-end JV to record June 2024 returns received after June 30, 2024 as a receivable and accrued revenue for FYE, noted in Key Control 3 for ATLAS, in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

## State of Washington

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all*



## State of Washington

*control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #3 - (Manual) - Valuation/Occurrence/Completeness** - The ATLAS "gross receipts" report, which is programmed to pull all gross receipts for the period July 1-August 15, is downloaded to Excel and compared to the gross receipts from the prior five years to ensure completeness. Revenue Accounting will prepare a JV to enter into AFRS to show the June returns received after June 30<sup>th</sup> as a receivable and accrued revenue for the FYE.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

We obtained the Gross Receipts 2024 Worksheets from Jerry, which included the gross receipts year-end accrual JV, see [[YE Accrual JV](#)], the gross receipts ATLAS report for filing period 6/30/24, see [[Accrual JV Testing](#)] (tab: ATLAS Gross Receipts Adj. 2024), and the taxpayer assessed taxes report, see [[Accrual JV Testing](#)] (tab: taxpayer assessed taxes) as well as detailed reports of gross receipts by taxpayer. We reviewed the gross receipts ATLAS report and noted that the amount for Sales tax (\$1,337,356,750.90), Use tax (\$64,085,813.64) and Business & Occupation (B&O) tax (\$560,782,602.91) tied to the taxpayer assessed taxes report. We reviewed the gross receipts year-end JV and tied the Sales, Use, and B&O tax amounts from the taxpayer assessed taxes report to the JV and ensured they occurred in the correct period. We noted that the JV was prepared by Andrew Arnold, Management Analyst, on 08/20/24 and approved by Melissa Russell, Accounting Manager, on 08/21/24. **No issues noted.**

**Noted Weaknesses are as follows:**

## State of Washington

- None.

### **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.2.PRG - Retail Sales and Use and B&O Taxes**

*Procedure Step:* Key Control # 4 (Manual)

*Prepared By:* BFW, 5/16/2024

*Reviewed By:* RKM, 8/5/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm monthly reconciliation between ATLAS and AFRS noted in Key Control #4 for ATLAS in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

## **Key Control #4 - Manual - Occurrence/Completeness for ATLAS**

At the end of each month, Revenue Accounting runs a monthly revenue activity report (MRA) from ATLAS and AFRS revenue report from Enterprise Reporting System. A reconciliation is then performed between ATLAS and AFRS to ensure the reported revenue and receivables amounts are accurate and complete.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

We met with Jerry Tilson, Revenue Accounting Manager, on April 10, 2024 via Teams to review the month-end reconciliation process performed between ATLAS and AFRS. We reviewed the February 2024 Monthly Revenue Activity spreadsheet. We noted the balances reported for the 1) Retail Sales tax \$1,111,963,612.59 2) Use tax \$75,835,876.76 and 3) Business and Occupation tax \$504,206,350.51 from each GL (Cash and Accrued Revenue) tabs from the ATLAS data and that the totals tied to the total under the "spreadsheet monthly activity" column on the "balance" tab. We also tied amounts included in the balance tab for the 1) Retail Sales tax 2) Use tax and 3) Business and Occupation tax directly to the WebI report without exception. There were no differences noted on the MRA spreadsheet between the ATLAS and AFRS data. ***No issues noted.***

### **Noted Weaknesses are as follows:**

- None

### **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **D.2.PRG - Retail Sales and Use and B&O Taxes**

*Procedure Step:* Risk Assessment

# State of Washington

*Prepared By:* BFW, 8/1/2024

*Reviewed By:* RKM, 8/5/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*
  - *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

## State of Washington

- *Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*
- *Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*
- *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*
  - *Are there substantial pressures or motivations to misstate the balance?*
- *Inherent Risk due to Misappropriation*
  - *Is the account balance or transaction class susceptible to sizable misappropriation?*
- *Inherent Risk due to Non-Compliance*
  - *Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*
  - *Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*
  - *Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

## State of Washington

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- **Occurrence - Moderate**
- **Completeness - Moderate**
- **Valuation - Moderate**



# State of Washington

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

- **Automated Tax and Licensing Administration System (ATLAS) - MAX - Occurrence, Completeness, Valuation**

We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

- **Occurrence - Moderate**
- **Completeness - Moderate**
- **Valuation - Moderate**

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

- **Occurrence/Completeness/Valuation** - We will perform analytical procedures and follow up on any significant variances.
- **Occurrence/Completeness** - We will select a sample of registered taxpayers, review ATLAS for a filed return, and tie return to AFRS to ensure revenue occurred in the current year and is complete.
- **Occurrence/Completeness** - We will select a sample of sales, use, and business and occupation accrual transactions from the gross receipts accrual JV and verify that the transactions were recorded for the correct period.
- **Valuation** - We will recalculate taxes paid for the same sample of taxpayers noted above to ensure taxes are recorded at proper values

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## **D.2.PRG - Retail Sales and Use and B&O Taxes**

*Procedure Step:* Substantive Test

# State of Washington

*Prepared By:* BFW, 10/15/2024

*Reviewed By:* SHW, 2/12/2025

## Purpose/Conclusion:

### **Purpose:**

To determine whether reported revenues represent actual amounts relating to the period.

To determine whether all revenues relating to the period were reported.

To determine whether revenues were reported at properly valued or calculated amounts.

### **Conclusion:**

We determined reported revenues represent actual amounts relating to the period, all revenues relating to the period were reported, and revenues were reported at properly valued or calculated amounts. ***No issues noted.***

## Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

- Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

- If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.
- Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.
- Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.
- Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

### **Cut-Off / Revenue Recognition**

- Test transactions recorded in the current period to verify the revenue occurred during the period.

*Transactions recorded at the beginning and end of the current period would generally be considered at highest risk of being improperly recorded in the current period. Consider scanning and selecting transactions if high risk transactions can be identified by description or*

# State of Washington

*date fields.*

- If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.
- Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

## **Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

## **Detail Roll-up**

- Compare year-end totals from general ledger to subsidiary software modules for selected revenues.
- Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the completeness assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

- Identify expected revenue streams based on understanding of fund activities and scan to see if revenue is reported for all such streams. Follow up on any unexpectedly missing streams.
- Identify new revenues (ex: new grants or programs) and follow up to verify that expected revenues have been reported.
- Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

- If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.
- Trace selected or sampled revenues from source documents to accounting records.

*Source documents may consist of billing, fine, or fee records. Or it may consist of service records that imply a billing, such as license or permit issuance.*

## State of Washington

- Perform a multi-year trend of revenues and follow up on unexpected decreases.
- Search for manual journal entries that debit (decrease) revenues. Consider testing if any risk indicators are noted.

### Cut-Off

- Test transactions recorded in the next period to determine whether the revenue should have been recorded in the current period.

*Transactions recorded at the beginning of the next period would generally be considered at highest risk of being improperly shifted to that future period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields. If the population is large, consider stratifying to either scan and select or test 100% of all large value transactions combined with a lower assurance sample for small dollar transactions.*

### Detail Roll-up

- Compare year-end totals from general ledger to subsidiary software modules for selected revenues.
- Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### Calculation

- Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.
- For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.
- Review related-party transactions to determine whether revenue transactions were correctly calculated.

### Realizable Value

- Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.
- Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.
- Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

# State of Washington

## Estimation / Recognition

- Review calculation and support for assumptions of any estimated revenues.
- Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

**Property Tax Revenues** - see separate step

Guidance/Criteria:

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

**BARS [3.6.13](#) Utility Tax (*applies only to cities*)** - should be accounted for as a revenue in the general fund (3164000) and expenditure in the utility fund (53P0040), if the utility passes the tax on to its customers then the additional charges should be recognized as revenue (343P000) directly in the utility fund not in the general fund

### **BARS [3.6.11](#) Suspense Funds**

Record of Work Done:

### **Retail Sales and Use and B&O Taxes Testing Coverage**

#### **Analytical Procedures**

We compared reported retail sales and use tax and B&O tax revenues against forecasted amounts to determine if amounts were within our expectations [[Tax Revenue Analytical](#)]. Based on historical experience, we expect the ERFC's June forecast to be within 3% of reported revenue for Sales tax and B&O tax.

Forecasted amounts were developed by the [Economic and Revenue Forecast Council \(ERFC\)](#), published on their public website, and used in the state's budget and operating processes. We determined that the forecast was sufficiently reliable to use as an expectation for our audit purposes. In making this determination, we noted the following about the competence, capabilities, and objectivity of ERFC staff and the objectives, intended use and methodology of ERFC forecasts:

## State of Washington

- ERFC is organized as a separate administrative board (S104) and is governed by both legislative and executive members and the State Treasurer. ERFC is organized and governed to be free from undue pressures or bias to ensure reliability of forecasts.
- The ERFC executive director is a Ph.D. in economics and staff consist of a group of economists. ERFC data and methodology is published on their website for transparency. ERFC is staffed to have the competence and capabilities to ensure production of consistently reliable forecasts.
- Four times a year the organization adopts a bipartisan revenue forecast that is then used to build the state operating budget. ERFC has demonstrated its reliability over time for this purpose. In prior state ACFR audits, we have found ERFC forecasts to be an accurate prediction of retail Sales, Use and B&O tax revenues.

We obtained the June quarterly revenue forecasts from the ERFC for FY 2024 and found that reported revenue was within 0.4% for both Sales and B&O taxes, which met our expectations. ***No issues noted.***

In addition to our analytical procedures, we also tested a sample of tax returns to obtain further evidence. Results of analytical procedures did not identify any needed adjustments or expansion to our sample or any further audit procedures.

### **Population**

To ensure testing provided a sufficient amount of coverage of the retail sales and use and B&O Taxes balance, we obtained our population for selection and broke out the taxes by fund and sources to ensure amounts we tested represented the whole balance. We obtained a query from ATLAS from Ayano Faasumalie, Revenue & Financial Reporting Coordinator, that included all payments applied to taxpayer accounts for excise taxes for the Fiscal year 2024, excluding those for local taxes. We tied the totals directly to the monthly revenue activity (MRA) spreadsheet prepared by Revenue Accounting at DOR and provided by Jerry Tilson, Revenue Accounting Supervisor. We used the MRA spreadsheet to break out each tax type by fund and source and tied amounts to the ACFR line item lead sheet [[Line Item Lead Sheet](#)]. See our reconciliation as part of testing at [[Tax Revenue Testing](#)], in tab 'Testing Summary.' Amounts tied without exception. We considered the population complete and provided coverage over the whole ACFR balance. ***No issues noted.***

Using the revenue query ran from ATLAS noted above, we haphazardly selected a sample of 30 transactions (payments made to a taxpayer account for a single filing period) and used the same sample to ensure amounts reported in AFRS occurred in the current year, are complete, and accurately valued. See more details for each assertion below.

### **Substantive tests performed to meet the Occurrence assertion:**

To ensure reported revenues represent actual amounts relating to the period, we performed the following substantive tests:

- Ensured return was filed for taxpayer
- Ensured tax revenue was recorded to batch processed in ATLAS for the correct period
- Ensured batch total processed in ATLAS ties to batch total recorded in AFRS

## State of Washington

For each selection, we reviewed the revenue tab within the taxpayer's account and history sub tab to identify the tax return for the correct filing period. Within ATLAS, a hyper link for the ATLAS receivable accumulation that the transaction was included could be followed from there. We traced each taxpayer account to the ATLAS accumulation and matched the batch total in ATLAS to the year end entry to AFRS using additional hyperlinks. Based on the tax type, we ensured the revenue was included in the correct balance. ***No issues noted.*** See testing performed at [[Tax Revenue Testing](#)] in the "Tax Revenue Testing" tab.

We also performed testing over the fiscal year end gross receipts accrual JV. See: [[Accrual JV Testing](#)]. No issues were noted during testing. We used the gross receipts detail report of taxpayer accounts to test the following:

- Did reported revenues actually occur during the fiscal year?

We selected a sample of 30 gross receipt transactions to ensure amounts reported in the current year were for revenues collected for the current year. We obtained tax returns and payment history tabs from ATLAS to ensure amounts were paid for taxes due in the current year. All taxpayers had a filing period of 6/30/2024. We determined all reported revenues occurred during the fiscal year. ***No issues noted.***

### **Substantive tests performed to meet the Completeness assertion:**

To determine whether all revenues relating to the period were reported, we performed the following substantive tests:

- Ensured return was filed for taxpayer
- Ensured tax revenue was recorded to batch processed in ATLAS for the correct period
- Ensured batch total processed in ATLAS ties to batch total recorded in AFRS

For each selection, we reviewed the revenue tab within the taxpayer's account and history sub tab to identify the tax return for the correct filing period. Within ATLAS, a hyper link for the ATLAS receivable accumulation that the transaction was included could be followed from there. We traced each taxpayer account to the ATLAS accumulation and matched the batch total in ATLAS to the year end entry to AFRS using additional hyperlinks. Based on the tax type, we ensured the revenue was included in the correct balance. ***No issues noted.*** See testing performed at [[Tax Revenue Testing](#)] in the "Tax Revenue Testing" tab.

We also performed testing over the fiscal year end gross receipts accrual JV. We reconciled the taxpayer accounts in gross receipts detail reports and the gross receipts revenue allocation work sheets, which allocates the funds held in the suspense account 01-99-020000 to the general fund revenue sources, to the year end accrual JVs for sales, use and business & occupation tax. See reconciliation of gross receipts detail report and the accrual JV as part of the testing at [[Accrual JV Testing](#)] in the "JV Accrual Summary" tab.

Amounts tied without exception and we determined the gross receipts recorded for sales, use and B&O taxes from the accrual JVs were complete. We used the gross receipts detail report of taxpayer accounts to test the following:

- Accrual recorded ties to tax return in ATLAS
- Accrual was recorded in the proper period

## State of Washington

We selected a sample of 30 random taxpayers to ensure amounts reported in the accrual JV were complete based on tax returns due. We tied all selected accrual transactions to tax returns without exception and noted payments were made in July and August for 2024 taxes due. We determined the accrual JV transactions were complete. ***No issues noted.***

### **Substantive tests performed to meet the Valuation assertion:**

To determine whether tax revenues were reported at properly valued or calculated amounts, we performed the following substantive tests:

- Recalculated retail sales, use, and B&O taxes for the selected taxpayer

During review of controls, we noted ATLAS automatically applies tax rates for retail sales, use, and B&O taxes and automatically calculates taxes due. To test the IT control, we re-performed calculations for a sample of 30 taxpayers as documented at [Tax Revenue Testing] in the "IT Control Testing - Valuation." We noted that all taxes recalculated tied to the taxes owed and paid in ATLAS and determined that revenues were reported at properly valued and calculated amounts. ***No issues noted.***

### **D.3.PRG - Deferred Inflows of Resources**

***Procedure Step:*** Summary & Conclusion

***Prepared By:*** BFW, 10/8/2024

***Reviewed By:*** RKM, 11/21/2024

Purpose/Conclusion:

#### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

#### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:



# State of Washington

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?

## State of Washington

- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

# State of Washington

## D.3.PRG - Deferred Inflows of Resources

*Procedure Step:* Understanding of Line Item

*Prepared By:* BFW, 5/22/2024

*Reviewed By:* CJG, 11/25/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associated with the line item.
- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and

## State of Washington

which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

There was a verbal recommendation in the prior year for DOR to record a review by DOR staff of each County's acceptance for the calculated Levy balance. During our understanding of contorts, we noted this was remedied by DOR documenting who from each County accepted and when this occurred.

#### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

# State of Washington

Deferred Inflows of Resources arise when a potential revenue does not meet both the "measurable" and the "available" criteria for revenue recognition in the current period. "Available" meaning the financial resources would be collectible within the current period or within 60 days. The Deferred Inflows balance is primarily from property taxes which make up approximately 67% of the line item, with the next largest amount composed of other taxes (33%) that will not be collected within 12 months.

## **Property Tax**

Property taxes are levied in December for the following calendar year. The first half-year collections are due by April 30 and the second half-year collections are due by October 31. Since the state is on a fiscal year ending June 30, the first half-year collections are recognized as revenue if collectible within 60 days of the fiscal year end. The second half-year collections are recognized as receivables offset by deferred inflows. The lien date on property taxes is January 1 of the tax levy year.

The legislature sets the rates of property tax amounts and DOR is responsible for calculating the amounts, but not setting them. DOR calculates the total amount due by all 39 counties by taking last year's levy amount and adding the mandatory increases. These include a base 1% or inflation (whichever is less), new construction value increases and any remaining balances.

## **Other Taxes**

We discussed the composition of the remaining balance with Ayano Faasumalie, DOR Revenue & Financial Reporting Coordinator, which is other taxes. She explained the unavailable reported under other taxes are based on receivable tax types from ATLAS. This includes: Return Receivables, Estimated Returns, Audit Receivables, and Lien Receivables. Based on collection rates identified by Revenue Accounting, DOR determines how much of the receivables will be collected within a year and the remainder would be recorded as unavailable for the current year. We gained an understanding of controls over receivables and collectible/uncollectible rates at [\[Controls - ATLAS\]](#).

We reviewed internal audit risk assessment documents for any significant changes in the processes and composition of the balance and noted no changes. We inquired with Jerry Tilson, Revenue and Accounting Manager, of any other changes he identified. He explained that the balance had no significant changes. **No significant changes or risks identified.**

## **(3) Updates to Significant Account Matrix:**

We identified no changes that need to be made to the Significant Account Matrix.

## **D.3.PRG - Deferred Inflows of Resources**

*Procedure Step:* Controls - PTRS

*Prepared By:* BFW, 5/22/2024

# State of Washington

*Reviewed By:* CJG, 11/25/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all significant systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

## State of Washington

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?

## State of Washington

- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **Significant Balance(s) and Assertions**

Internal controls in Property Tax Receivable System (PTRS) address the following balance(s):

- **Deferred Inflows of Resources** - General Fund

For the following assertions:

- **Classification** - Revenue may be recorded as earned when it is actually unearned (availability criteria is not met).

### **Gain an Understanding of Internal Controls**

We identified property tax as the majority of the deferred inflows of resources balance (67% of the prior year balance) and will be focusing our understanding of controls over this area. We met with Mark Studer, Tax Policy Specialist, Research and Fiscal Analysis (RFA), on May 15, 2024 to gain an understanding over property tax certified levy calculation.



# State of Washington

For fiscal years 2018 through 2021, the agency used rate based levy calculations to determine levy amounts for counties. This change was a direct result of the McCleary ruling which required the State of Washington to fund schools. In a rate based system, the rate is set and multiplied by the assessed values of property to result in the levy amount. In fiscal year 2022, the agency returned to the budget based system for both part 1 and part 2 state school levies and this remained the case for FY24. In the budget based system, the amount of levy collections is limited and set by the State and allocated to counties based on the market value of all taxable property in the county.

## **State Property Tax Levy Calculation:**

Mark explained that levies are increased on an annual basis but are limited by a few things. These increase limits include the following:

- The lesser of 1% or inflation
- The value of new construction multiplied by the prior year rate
- The value of state assessed properties (properties owned by utilities such as airline, railroad, and electric) multiplied by the prior year rate

Research and Fiscal Analysis (RFA) will use the prior year levy limit and add the above increases to result in the current year state levy limit. The new levy limit is the amount used and proportioned to counties.

In October/November, counties submit assessed value reports to DOR which the RFA division inputs in an excel sheet to use in their calculation of the levy rates for the current year. However, DOR does not use the unadjusted assessed values from the county, instead, the property tax division will perform a ratio analysis to identify ratios for each county's real and personal property. These ratios are used to adjust the assessed values to actual (market value) for both local and state assessed properties. RFA divides the current year state levy limit (described above) by the actual value for all counties to determine the new rate to be used for the calculation of levy amounts.

Each year, RFA will have to make adjustments to county levy amounts for changes identified in the prior year. Most of the changes stem from differences in assessed value from the time they are submitted to the time that the counties distribute the levies. These changes are included in the next year's calculation to reduce the amount of adjustments made throughout the year. All adjustments are the following:

- Fifth Preceding Year Adjustment - The remaining balance not collected from the fifth preceding year is rolled into the current levy amount. For example, 2019 is the fifth preceding year for fiscal year 2024; therefore, any amounts remaining in 2019 will be "rolled" over and counties will not be required to pay on the remaining balance for 2019 as it will have been rolled over/included in the total state levy amount to be collected for fiscal year 2024.
- Refund Levy Adjustment - When a taxpayer pays while in dispute with amounts owed and the court rules in their favor, amounts are refunded. DOR increases the next year's levy amount to ensure the total levy balance from the prior year is collected.
- Previous Year's Levy Adjustment - Due to changes in assessed value from the point they are submitted to DOR to the point the levies are distributed by the county (April-May). The counties will send an update of assessed values when the levies are distributed. DOR uses these updated assessed values to calculate adjustments for the next year.

RFA has several review processes to ensure calculations are accurate for the state levy. First, RFA creates an assessor review tab within the state

## State of Washington

levy calculation spreadsheet that includes the assessed values of all counties that were submitted. To ensure the amounts input and used for calculations are accurate, RFA asks the counties to verify the assessed values to their own records. Mark Studer, Tax Policy Specialist, prepares the entire state levy calculation spreadsheet. He explained that a secondary reviewer will ensure calculations are consistent with prior years and are allocated appropriately.

In December of each year, county assessors receive a letter from DOR regarding the state property tax levy amount due in the upcoming year for part 1 and part 2. The letter is automatically generated to include the calculations and adjustments noted above. Before the letters are sent, 2 separate members of the Property Tax Division select a random sample of letters to ensure amounts sent to the county agree to the calculations. The most important figure, the total state levy owed by the county, is bold and circled in red so the counties are aware of their allocated amount. The county will determine its own levy rate by dividing the state levy amount by their own assessed value of property. Since the assessed value is less than the market value used by DOR in their calculations of the levy rate, the county's levy rate will be slightly higher. Once the county agrees no changes need to be made, DOR records the review by each county in the "review" tab of the "State Levy Documents Received" spreadsheet and stores the email in a communal mailbox. The valuation control for Deferred Inflows of Resources consists of each county verifying the calculated amount of Levy due is consistent with previous years and county changes in valuation. When the county agrees to the total calculated, it is generally sent in an email and added to a communal inbox that can be reviewed by members of DOR. However, it is not a requirement that the acceptance be submitted in writing as some counties prefer to communicate over the phone. DOR keeps track of county acceptance in their "State Levy Documents Received" spreadsheet, noting who from each County confirmed and accepted and when this occurred.

### **Property Tax Collections:**

We met with Jerry Tilson, Revenue Accounting Manager, on May 22, 2024 to gain an understanding over Deferred Inflows reporting. The 39 counties, not DOR, are responsible for collecting property taxes; however, the tax revenue and cash received are recorded by DOR in AFRS. Per Andrew, DOR uses the Property Tax Receivable System, a web-based database, to track property tax collections by county. The web-based database is a more practical means for running summary reports rather than AFRS.

Counties remit taxes they collect to the Office of the State Treasurer (OST) using a cash journal (CJ). OST summarizes these individual CJ's into a JV and records the cash into AFRS. Using the county cash journal (CJ), the Revenue section of DOR's Business and Financial Services records the information into spreadsheets and the Property Tax Receivable System to track collections by county. Expected collections (the State Property Tax Levy of 2023 expected to be collected in 2024) are input into the Property Tax Receivable System (PTRS) by a Fiscal Analyst 2 and verified by Jerry Tilson, Revenue Accounting Manager. Using the OST JV, DOR's Revenue Accounting prepares a JV and records the revenues into AFRS by revenue source. A Cash Receipts Journal Summary is prepared for each county's total deposits and sent to the Office of the State Treasurer, this is done prior to any adjustments.

### **How transactions are recorded in AFRS (Year-end JV):**

At year end, a Property Tax Accounts Receivable summary report is run of the total Property Tax Receivable System as of June 30 (GL 1311). It is a running total of taxes due by county for the preceding five years 2017-2021. Estimated collections for July and August are provided by the

# State of Washington

Forecast Council and are included in the year-end adjusting entry. The forecasted amounts are based on the June forecast and total approximately 2% of the total receivables.

A year-end journal voucher for unavailable property tax revenue is prepared by a Fiscal Analyst 3 by subtracting the estimated collectible amounts for July-August (as received from the Forecast Council) from the year end property tax account receivable report. This Journal Voucher is reviewed by a fiscal analyst 5 to ensure deferred inflows of resources is properly calculated. The supervisor/manager reviews all the supporting documentation that was used by the fiscal analyst in preparing the JV to ensure the amount reported is accurate and classified correctly based on forecast information **(Key Control 1- Classification)**.

## **Monthly Reconciliations:**

A monthly reconciliation of AFRS to the web-based data base for property taxes is performed each month. An Exception Ending Balance report is used to track differences between the Accounts Receivable amount and the Ending Balances. The expectation is previous month's ending balance minus the current month's payments, plus or minus adjustments (typically corrections to sub source) is what is recorded. Any negative balance for an individual levy year does not reduce the amount of the receivable for the combined levy years. In addition, reconciliations are performed by Andrew each month of cash payments made per the PTRS and the monthly balance per AFRS. Monthly Journal Vouchers are received from OST documenting the transfer of monies remitted by the counties to DOR during the month. A spreadsheet is prepared to document and reconcile the cash receipts journal summary to OST's monthly JVs to ensure collections are classified appropriately **(Key Control 2 - Classification)**.

## **Key controls are as follows:**

- **Key Control 1 - Classification - The Fiscal Analyst 3 prepares the year end entry to record deferred inflows of resources using PTRS accounts receivable reports and Forecasts from the Forecast council. The Fiscal Analyst 5 reviews supporting documentation to ensure amounts are accurate and classified correctly based on forecast information.**
- **Key Control 2 - Classification - Jerry Tilson, Revenue Accounting Manager, reconciles Property Tax Receivable System (PTRS), AFRS, and OST JVs on a monthly basis to ensure collections are classified appropriately.**

## **Noted Weaknesses are as follows:**

- none

## **D.3.PRГ - Deferred Inflows of Resources**

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* BFW, 10/7/2024

# State of Washington

*Reviewed By:* CJG, 11/25/2024

Purpose/Conclusion:

**Purpose:**

To confirm the year end JV to record the unavailable tax revenue in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

## State of Washington

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

## State of Washington

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 1 - Classification - The Fiscal Analyst 3 prepares the year end entry to record deferred inflows of resources using PTRS accounts receivable reports and Forecasts from the Forecast council. The Fiscal Analyst 5 reviews supporting documentation to ensure amounts are accurate and classified correctly based on forecast information.**

The understanding for this system is documented above in the "Controls - PTRS" step.

### **1. Confirmation of Key Manual Control:**

Jerry Tilson, Revenue Accounting Supervisor, provided the AFRS journal voucher and Property Tax Receivable System report and taxes receivable forecast used to record the year end JV.

There is a one month delay between when counties collect the taxes and when they are submitted to DOR, so DOR's taxes receivable balance as of June 30th is the counties balance as of May 30th. Jerry provided the Counties May Accounts receivable balances through screenshots of PTRS for Part I and Part II. He also provided the forecast council's excel sheet that tracks all receivables "Forecast Allotment\_2325\_2024\_06" as of June 30th. Property taxes are listed on the "2325 Cash Jun 2024" tab, in lines 11 and 12 (source code 50, subsource code 02: Property Tax) for parts I and II respectively. Columns 01 and 02 are the first two fiscal months. Altogether, there are four balances pulled from this spreadsheet for the two parts of the levy in the first two fiscal months, that all together makes the estimated available property tax revenue. Jerry provided the

# State of Washington

property tax estimates in a simplified table "Property Tax Forecast for FY25"

We reviewed the JV 14030885 and noted \$2,237,257,889.58 was recorded as unavailable revenue (deferred inflows of resources) 5192. The JV was prepared by Andrew Arnold, Fiscal Analyst, on July 23, 2024 and reviewed by Jerry Tilson, Revenue Accounting Supervisor on July 23, 2024. We vouched the recorded JV amount to Property Tax Receivable system reports less the estimated collections for the current year for both part 1 and part 2 of the levies. ***No issues noted.***

## **Noted Weaknesses are as follows:**

- None.

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **D.3.PRG - Deferred Inflows of Resources**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* BFW, 5/22/2024

*Reviewed By:* CJG, 11/25/2024

Purpose/Conclusion:
---------------------

## **Purpose:**

To confirm monthly reconciliations between OST JVs and the cash receipts journal summary in order to assess control risk.

# State of Washington

## **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*



## State of Washington

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 2 - Classification -Jerry Tilson, Revenue Accounting Manager, reconciles Property Tax Receivable System (PTRS), AFRS, and OST JVs on a monthly basis to ensure collections are classified appropriately.**

The understanding for this system is documented above in the "Controls - PTRS" step.

### **1. Confirmation of Key Manual Control:**

Monthly journal vouchers are received from OST documenting the transfer of monies remitted by the counties to DOR during the month. A spreadsheet is prepared to document and reconcile cash receipts journal summary to OST's monthly JVs.

Jerry Tilson, Revenue Accounting Manager, provided the March 2024 reconciliation. We reviewed the Property tax part 1 March reconciliation and tied the Property Tax Receivable System (PTRS) ending balance for Clallam County to PTRS accounts receivable reports. Per PTRS the ending balance was \$21,214,147. The OST cash journal entries totalled \$2,998,537 for the month. The prior month ending balance of \$24,212,684 less the March cash receipts resulted in an ending balance of \$21,214,147 per the source documents from OST. No variance was noted for any of the counties between PTRS and OST JVs. ***No issues noted.***

Revenue Accounting performs a reconciliation between PTRS and AFRS to ensure that payments received are accurately reported and classified appropriately. We noted the total payments for all counties for March were \$140,263,300.23 as documented in PTRS. We tied this amount to AFRS using an ER report for General Fund source 50 - property tax. Amounts tied without exception. ***No issues noted.***

### **Noted Weaknesses are as follows:**

- None.

# State of Washington

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.3.PRG - Deferred Inflows of Resources**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* BFW, 5/22/2024

*Reviewed By:* CJG, 11/25/2024

Purpose/Conclusion.:

#### **Purpose:**

To confirm monthly reconciliations between OST JVs and the cash receipts journal summary in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy.:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls*

## State of Washington

*were consistently and effectively applied).*

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

**Key Control 2 - Classification - Jerry Tilson, Revenue Accounting Manager, reconciles Property Tax Receivable System (PTRS), AFRS, and OST JVs on a monthly basis to ensure collections are classified appropriately.**

The understanding for this system is documented above in the "Controls - PTRS" step.

## **1. Confirmation of Key Manual Control:**

Monthly journal vouchers are received from OST documenting the transfer of monies remitted by the counties to DOR during the month. A spreadsheet is prepared to document and reconcile cash receipts journal summary to OST's monthly JVs.

Jerry Tilson, Revenue Accounting Manager, provided the March 2024 reconciliation. We reviewed the Property tax part 1 March reconciliation and tied the Property Tax Receivable System (PTRS) ending balance for Clallam County to PTRS accounts receivable reports. Per PTRS the ending balance was \$21,214,147. The OST cash journal entries totalled \$2,998,537 for the month. The prior month ending balance of \$24,212,684 less the March cash receipts resulted in an ending balance of \$21,214,147 per the source documents from OST. No variance was noted for any of the counties between PTRS and OST JVs. ***No issues noted.***

Revenue Accounting performs a reconciliation between PTRS and AFRS to ensure that payments received are accurately reported and classified appropriately. We noted the total payments for all counties for March were \$140,263,300.23 as documented in PTRS. We tied this amount to AFRS using an ER report for General Fund source 50 - property tax. Amounts tied without exception. ***No issues noted.***

## **Noted Weaknesses are as follows:**

- None.

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

# State of Washington

## D.3.PRG - Deferred Inflows of Resources

*Procedure Step:* Substantive Test

*Prepared By:* BFW, 10/8/2024

*Reviewed By:* CJG, 11/25/2024

Purpose/Conclusion:

**Purpose:**

To determine whether financial statements properly classify deferred inflows of resources in conformity with generally accepted accounting principles (GAAP).

**Conclusion:**

We determined reported deferred inflows were correctly classified. ***No issues noted.***

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

## State of Washington

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the **Permanent File** folder or assessment of control risk?
  - If circumvention, the **Management Override of Controls** step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate



## State of Washington

evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

### **Substantive tests performed to meet the Classification assertion:**

To ensure deferred inflows of resources were classified correctly within PTRS, we selected a sample of monthly cash journals prepared by the Office of State Treasury to review. To determine whether the property taxes were correctly classified, we recalculated the year-end JV and tied totals to the source codes.

### **Classification Testing Results:**

To determine whether the property taxes were correctly classified, we obtained the year end JV. We deducted the collections expected within 60 days and identified the unavailable revenue as the receivables that will not be collected within that time, see testing here: [[FY24 Year End JV Testing](#)]. Our determination tied to the year end JV without exception. *No issues noted.*

To ensure deferred inflows of resources were classified correctly within PTRS, we selected a sample of monthly cash journals prepared by the Office of State Treasury. We selected five journal vouchers and two individually significant vouchers that represented 97.97% of all collections for the year, to review for the following:

- Property Tax Collections are recorded in proper revenue source codes in PTRS (Property Tax Receivable System)
- Property Tax Collections recorded by OST cash receipt journal summaries into AFRS are coded correctly.

We reviewed the source coding on the county's A8s and the compiled OST monthly JVs to ensure the balances remitted were entered into the correct codes; Fund 001, Source 0150, Subsource 020000 and 020001. We determined the the OST JVs and the PTRS records were coded correctly without exception. See testing here [[Property Tax Collection Testing](#)] on the JV Testing tab.

**In addition, we addressed the existence/completeness assertion in this area as this testing will be used for part of the coverage of the taxes receivable balance testing.**

**Substantive tests to meet the Existence assertion (Relevant to the Taxes Receivable testing only):**

## State of Washington

We traced each of the counties in the selected cash journals from OST to their A8s and their acceptance of the balance.

### **Existence Testing Results:**

We reviewed the A8 from each county for each of the months selected by the JV selection process. The A8s listed all the taxes collected by the county to be remitted to DOR through OST. We added the taxes collected from Fund 001, Source 0150, subsources 020000 and 020001 only for the amount of property tax collected. We added the totals of all 39 counties for the property taxes collected, and compared to the amount remitted to DOR through OST in the relevant JV under the same subsource codes. The total remitted to OST by all the counties matched the total remitted by OST to DOR. See testing here [[Property Tax Collection Testing](#)] on the JV Testing tab.

### **Substantive tests to meet the Completeness assertion (Relevant to the Taxes Receivable testing only):**

We added all the levy totals given to the counties and the total matched what the original total was (the same as last year plus 1% and adjustments)

### **Completeness Testing Results:**

Jerry Tilson, Revenue Accounting Manager, provided the letters sent to each of the 39 counties, which outlined the amount of property taxes due for Parts I and II in 2024. We totaled the amounts due from each of the counties for both parts. We compared the total of the letter amounts, to the total of all county levies as calculated in the State Levy spreadsheet. Both Parts I and II balanced. See testing here [[Property Tax Collection Testing](#)].

### **D.4.PRG - Human Services**

*Procedure Step:* Summary & Conclusion

*Prepared By:* AMG, 11/15/2024

*Reviewed By:* RKM, 11/20/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

# State of Washington

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

## Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

# State of Washington

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

Results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

# State of Washington

The quality and quantity of evidence obtained was sufficient and appropriate.

## D.4.PRG - Human Services

*Procedure Step:* Understanding of Line Item

*Prepared By:* AMG, 7/8/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

## State of Washington

- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update to Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

We reviewed the most recent audits or in-process audits for the agencies for accountability, SWSA, and ACFR for exceptions related to the Medicaid program:

## State of Washington

- ACFR Audits: Prior finding/management letters related to the general IT control deficiencies due to the lack of a SOC II type 2 report that addresses an entire year (even fiscal years have six months of coverage) or at all (odd fiscal years).
  - We will be reviewing the controls and follow up on this issue during the audit.**Impact:** This impacts our assessment of control risk for all assertions by increasing it to MAX as necessary.
- Single Audit: We reviewed the FY23 SWSA (S1Medicaid-SA23) for issues that directly correlate with our tested management assertions:
  - Provider Eligibility - Both agencies did not have adequate controls to ensure provider eligibility requirements for the Medicaid Program.
    - HCA relied on automated systems to assist in the revalidation of providers (required every five years); however, we noted that out 347 providers that should have been revalidated or deactivated: None were revalidated before the due date.
      - HCA subsequently revalidated 127 providers which were backdated
      - The remaining 192 providers should have been deactivated, but HCA did not take effort to deactivate or revalidate them
    - DSHS relied on automated systems to confirm the identify and exclusion status of providers, which is required monthly. A management decision was made to only screen providers on an annual basis. There was additionally missing documentation related to enrollment determinations.**Impact:** This impacts the Rights and Obligations assertion to ensure claims are paid to eligible providers at the time of service. When we met with SA for coordination [[ACFR / SWSA Brainstorm](#)], Stephanie Garza and Ronni Copeland mentioned that our methodology of testing eligibility was appropriate due to HCA's ability to backdate revalidations. We will continue to clarify with the Single Audit team during testing to ensure that our work addresses the requirements of the Medicaid portion of the single audit.
- Accountability/IT Audit: In FY23, we did not preform an accountability audit. There are no potential impacts to effect the audit.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

Final Coverage Analysis [[FY24 Human Services Breakdown](#)]

### **Expenditure Analysis**

We analyzed expenditures\* in the following manner [[FY24 Human Services Breakdown](#)].

- By Origin Code:
  - 83.99% of the expenditures for HCA were from ProviderOne (OC P1), presenting the most significant origin system. This is expected as ProviderOne is the Medicaid MMIS.
  - 43.22% of the expenditures for DSHS were from ProviderOne and 13.97% were from payroll (OC PR, which is addressed in other testing procedures in the ACFR).

## State of Washington

- By Subobject:
  - **HCA:** 94.43% were from NB (direct payments to providers)
  - **DSHS:** 81.52% were from NA/NB (direct payments to providers and clients)
- By GL Account
  - The only item related to the GL accounts is for GL 6525 for DSHS. This account is used for SNAP expenditures. This represented 23.29% of their expenditures.

These expenditures sources are all in line with our expectations due to the significance of the Medicaid program.

Based upon the quantitative and qualitative aspects of the Medicaid program, we do not consider identified changes to the expenditures significant which fluctuate year-to-year based upon actual services rendered and demand.

\*Note: The amounts within the analysis are interim and based upon the funds, GL accounts, and subobjects from FY23 ACFR queries which provide information between the income statement sort codes and AFRS transaction detail. We anticipate these are similar year-to-year and sufficient for preliminary analysis purposes. Additionally, based upon historical testing, we expect HCA and DSHS (followed by DCYF) to contribute the most to the Human Services line item as they are the primary agencies responsible for human services.

### **Amendment Updates**

The State Plan which describes the nature and scope of Washington's Medicaid Program is changed with plan changes (State Plan Amendments, SPA) submitted to the Department of Health and Human Services, to be approved by the Centers for Medicare and Medicaid Services (CMS) to determine whether it meets federal requirements and policies. The State Plan is updated when CMS issues final approval of an SPA.

We reviewed approved SPAs with approval dates within FY24 documented at [\[FY24 SPA Review\]](#). During our review, we noted general updates including extending/increasing of existing rates, technical changes and updates, and exceptions to existing procedures.

### **Testing impact assessment:**

- **Valuation** - We identified multiple rate and effective date updates within the SPAs. Correct rates are an attribute for testing and a sample of rate updates for accuracy and review and upload process is tested as part of control testing [\[Key Controls #1 - 4 Edit Checks \(Automated\)\]](#).
- **Completeness** - We identified SPAs that would increase the number of eligible clients through various means. This has no impact on our testing as we test for "negative" attributes, i.e. if the client was eligible at the time of service, rather than should more clients have been registered as eligible. There is no financial impact for "potentially eligible" clients as they do not submit claims if they are not registered.

### **Public Health Emergency End [\[WAH Guide to Unwinding\]](#)**

During the Public Health Emergency (PHE), CMS provided guidance that allowed for relaxed eligibility determinations and redeterminations, known



## State of Washington

as the continuous enrollment provision. Essentially, enrollees were allowed to self-attest to their conditions and income levels for their eligibility into their recipient aid groups. Those that had coverage were able to retain their coverage throughout the PHE. The PHE ended on 5/11/2023, but the Consolidated Appropriation Act of 2023 ended the provision. HCA and DSHS resumed normal operations for eligibility redeterminations 4/1/2023, with terminations for those that did not renew eligibility resuming on 5/31/2023.

During this time period, HCA began its efforts to reach clients, including phone calls, text messages, mail/enhanced envelopes, and updated correspondence for clients to respond to renewals and eligibility reviews to determine if they were still eligible for Apple Health coverage or other insurance through the Washington Healthplanfinder. Depending upon the coverage group (Classic Apple Health coverage through DSHS, MAGI Apple Health through Washington Healthplanfinder, etc.) the redetermination process can either be automatic (comparing self-reported income through the Healthplanfinder to various sources) or a manual process.

One key takeaway, however, is that terminated clients have 90 days from their termination date to complete their renewal and have **retroactive reinstatement** from their termination date without a gap in coverage (**pg. 15**).

### **Testing impact assessment:** Potential impact

- **Rights and Obligations** - For those individuals who may be ineligible to receive services due to termination between the time frame of 6/1/2023 through 6/30/2023. As noted above and in the wind down guide, those terminated clients have an additional 90 days from termination to complete their renewal process for retroactive reinstatement. Eligibility of clients are still updated through batches from ACES to ProviderOne; we will take additional consideration for those TCNs that do not meet client eligibility on a service date to consider retroactive reinstatement.
- **Valuation** - HCA should potentially have a Expenditure Accrual estimate, with a corresponding Accounts Payable entry, for those clients (and their transactions) that are initially deemed ineligible due to the renewal lapse, but receive retroactive eligibility within the 90 day window. Per inquiry with HCA we determined this is not a new process in eligibility and has been in place since the enactment of the ACA. A client has up to 90 days to be reconsidered for their renewal and HCA can reinstate coverage back to termination. Once eligibility is established, claims can be submitted.

We identified during FY24 the Authority is still in the wind down period. The testing impacts that are assessed for FY24 would be considered an Eligibility risk however, this has trivial impact on financials due to the 90 day window for terminations.

### **SAO Risk Register**

We reviewed the Medicaid Task Force's Risk Register for topics that may impact the ACFR for our selected management assertions. We noted that the risks topics identified could more adequately be covered in other audits such as accountability and performance audits, rather than for financial reporting purposes.

### **(3) Updates to Significant Account Matrix:**

## State of Washington

We made a slight change to the DSHS line item risk to also include "A lack of service organization's internal control audit for the ProviderOne system could lead to inaccurate payments, misuse, loss of misuse, loss or misappropriation of public funds, or payments not properly made only to eligible recipients for allowable (authorized) services". The risks now match HCA.

No other updates to the Significant Account Matrix are necessary. Expenditures for the line items are in expected agencies and sub-objects. We did not identify significant changes in the expenditures from year to year.

### D.4.PRG - Human Services

*Procedure Step:* Controls - ProviderOne

*Prepared By:* AMG, 8/8/2024

*Reviewed By:* RKM, 12/2/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.

## State of Washington

- Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
- Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
- Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

## State of Washington

- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria.7
---------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

# State of Washington

Record of Work Done:

## **Significant Balance(s) and Assertions**

Internal controls in ProviderOne address the following balance(s):

- Statement of Activities - Government Wide - Human Services - Expenses
- Statement of Revenues, Expenditures, and Changes in Fund Balances - Governmental Funds - Human Services

For the following assertions:

- Rights and Obligations - Medicaid / social service payments may not be made to eligible providers, for eligible recipients, or for allowable services
- Valuation - Medicaid / social service payments may not be made at correct rates.
- Completeness - Payments may not be completely rolled-up to AFRS from P1.
- General Risk - ProviderOne is the Medicaid payments system. A lack of service organization's internal control audit for the ProviderOne system could lead to inaccurate payments, misuse, loss of misuse, loss or misappropriation of public funds, or payments not properly made only to eligible recipients for allowable (authorized) services.

## **Gain an Understanding of Internal Controls**

We met with the following to discuss ProviderOne and controls:

- Will Sogge, Audit Liaison
- Ed Hicks, IT System Administrator - Senior
- Heidi DeVries, IT Quality Assurance

### *Background:*

The Social Security Amendments of 1965 created Medicaid by adding Title XIX to the Social Security Act, 42 USC 1396 et seq. Under the program, the federal government provides matching funds to States to enable them to provide medical assistance to residents who meet certain eligibility requirements. The objective is to help States provide medical assistance to residents whose incomes and resources are insufficient to meet the costs of necessary medical services. Medicaid serves as the nation's primary source of health coverage for low-income populations.

Services are provided to Medicaid eligible enrollees either through enrollment in the managed care program or on a fee-for-service basis. Most medical services are provided by Medicaid providers. Medicaid providers can be any person, group of people, or health care facility that supplies medical services to Medicaid recipients. Providers include doctors, medical equipment companies, podiatrists, dentists, licensed professional counselors, hospitals, adult day care centers, nursing homes, clinics, pharmacies, ambulance companies, case management centers, home health care workers, and others.

### *Managed Care*

# State of Washington

Managed care is a prepaid, comprehensive system of medical and health care delivery. It includes preventive, primary, specialty and ancillary health services. The term "managed care" is used to describe a variety of techniques intended to reduce the cost of providing health benefits, improve the quality of care and deliver health care organized around managed care techniques and concepts. HCA administers the following managed care programs:

## *1. Apple Health (formerly known as "Healthy Options") managed care*

The majority of Medicaid clients are enrolled in the Apple Health program. The state pays a fixed rate (capitation rate) to licensed health insurance carriers to provide a defined set of services to enrolled members. Thus, these carriers are paid a negotiated capitation monthly premium without regard to the actual medical services utilized by each beneficiary. Clients in Apple Health managed care must see only providers who are in their plan's provider network, unless prior authorization is given or to treat urgent or emergent care.

Currently, the following five plans are available through the Apple Health managed care program:

- Wellpoint Washington (previously Amerigroup)
- Community Health Plan of Washington
- Coordinated Care of Washington
- Molina Healthcare of Washington
- United Healthcare Community Plan

## *2. Integrated Managed Care (known as "Fully Integrated Managed Care (FIMC)")*

FIMC coordinates physical health, mental health, and substance use disorder treatment services to help provide whole-person care under one health plan. Integrated managed care is available in all regions.

## *3. Apple Health Foster Care (AHFC)*

The Apple Health Foster Care (AHFC) program provides integrated managed physical and behavioral health coverage statewide to Apple Health children in foster care. Care coordination for all Washington State foster care enrollees is provided through a single, statewide managed care plan called Apple Health Core Connections administered by Coordinated Care of Washington (CCW). Apple Health children in foster care (out of home placement) are auto-enrolled to Coordinated Care of Washington.

## *4. Primary Care Case Management (PCCM)*

The Primary Care Case Management (PCCM) program is available for American Indians or Alaska Natives. The State's PCCM program is provided only through tribal clinics and Urban Indian Centers.

# State of Washington

## Fee-for-service

Under the fee-for-service delivery system, HCA pays providers directly for each service, using the ProviderOne payment system. Regardless whether a Medicaid client is enrolled in a managed care plan, the following services are always covered as fee-for-service (FFS):

- Dental Care
- Vision hardware (children only)
- Long-term care
- Inpatient psychiatric care for physician services.

Fee-for-service providers have agreed to accept the rates established by HCA as total payment for services. They are not permitted to bill clients for any amount above that which it received from HCA. For services in which there has been no designated rate, prior approval must be obtained before the service can be provided. HCA maintains several toll free lines for such approvals.

## **ProviderOne**

ProviderOne (P1) is the state's Medicaid Management Information System (MMIS). P1 is critical to the Medicaid program, processing claims transactions and payments for Medical, Social Services, Dental, and Pharmaceutical claims. The Health Care Authority relies on P1 for compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Medicaid (Title XIX). The Health Care Authority (HCA) contracted with a vendor, Client Network Services, Inc. (CNSI), to develop ProviderOne to process state Medicaid payments.

- Since May 9, 2010, P1 has been processing payments for managed care, hospital, medical, dental, medical supplies, vision, and nursing home claims in "Phase 1".
- Since January 15, 2015, social service provider payments, such as adult family home, assisted living home and home care agency claim payments, have been processed through ProviderOne instead of the Department of Social and Health Services' (DSHS's) Social Services Payment System (SSPS) in "Phase 2". Additionally, W2 social service provider payments were transferred from SSPS to IPOne, a new online billing system for W2 providers, as of March 2016. W2 provider payments, such as self-employed individual provider payments, have been processed through IPOne instead of the Social Services Payment System (SSPS) since March 2016.

The P1 system comprises the following subsystems:

- **Client** - Client information. Interfaces with DSHS's Automated Client Eligibility System (ACES), DSHS's Comprehensive Assessment Reporting Evaluation (CARE) system for Social Services Claims, and Department of Corrections' (DOC's) OMNI system for incarcerated individuals.
- **Provider** – Provider enrollment and validation. Interfaces with LexisNexis for provider screening and DSHS's Agency Contract Database (ACD).
- **Third Party Liability** - This subsystem is used when a client has other medical coverage and Medicaid is not the primary payer of the claim.
- **Prior Authorization** - This subsystem contains prior authorizations that are required for some medical services.

## State of Washington

- **Social Services** - This subsystem includes services provided by Home and Community Services Providers (individual and agency providers) and Residential Care Providers (adult family homes, nursing homes, etc.) who contract with DSHS. Almost all of the expenditures processed in this subsystem are recorded as DSHS expenditures because they fall under programs administered by DSHS. All social services should be pre-authorized. A social services' case worker will evaluate each client and determine what services will be provided to the specific client and will pre-authorize the services. P1 will not pay for social services that are not pre-authorized. The adjudication process is the same as other claims.
  - Prior to 6/1/2022, DSHS was the legal employer of and submitted claims information for individual providers. As of 6/1/2022, the Consumer Direct Care Network Washington (CDWA) is the legal employer of all Individual Providers (IP) in the state of Washington and is responsible for submitting claims for the individual home care providers.
- **Claims** – facilitates submission of claims, payment of claims, managed care payments/encounters, adjustments.
  - FFS and Managed Care claims
  - Edit processing
- **OFIN (Oracle Financials)** - used to store GL, A/P, A/R and other financial information.
- **Rate Setting** - HCA's Managed Care unit contracts with actuaries to determine rate. The actuary determines base rate for MCO and adjustment factors based on gender, age, location. P1 calculates actual rate based on the base rate and relevant actuary factors.

### Claims:

Payments initiated from ProviderOne can originate from two different subsystems: Claims and Managed Care. Medical or social service claim payments to providers are processed through Claims, managed care monthly premiums are paid to Managed Care Organizations through Managed Care. Premium assistance is paid to insurance organizations or clients through TPL.

P1 has hard coded edits to adjudicate medical/social service claims and managed care monthly premium payments. Using the details included in a claim, system edits will verify eligibility and allowability of the claim based upon related information included in P1 subsystems, such as Client, Provider, etc. Payment will not be made unless claims pass the hard edits. The adjudication process can be seen as summarized by the following flow chart: [\[Claims Adjudication Flow Chart\]](#).

Some of the key attributes of a claim that are checked by the edits include:

- The provider is eligible to provide the specific service covered by the plan to the specific beneficiary (**Key Control #1 (Automated) - Provider Eligibility, Rights and Obligations**)
- The beneficiary is eligible for the particular category of service at the time it was rendered (**Key Control #2 (Automated) - Beneficiary Eligibility, Rights and Obligations**)
- ProviderOne Verifies that the allowed amount is within reasonable and acceptable limits or if it differs from the allowable fee schedule amount by more than a certain percentage (**Key Control #3 (Automated) - Valuation**)
- The procedure codes are within the valid code set HIPAA Transactions and Code Sets (TCS) and are covered by the State Plan (**Key Control #4 (Automated) - Valid Codes, Rights and Obligations**)



# State of Washington

The ProviderOne system automatically provides daily reports to both the CNSI operations staff and HCA regarding the previous day's adjudication and processing results. In addition, weekly and monthly reports are provided to HCA. These reports provide indicators that processing is completed successfully and the results are within normal operating parameters. For example, claims denied percentage should not typically exceed paid percentage. Any usual variances in values would provide indications to the CNSI and HCA claims team that a possible problem may exist.

## Managed Care:

HCA contracts with managed care organizations (MCOs) to pay providers for Medicaid services to eligible Washingtonians. MCOs deliver defined benefit packages to eligible clients for fixed monthly rates determined by an independent actuary. ProviderOne pays the MCOs premiums for clients enrolled in Managed Care Programs (MCP).

Managed Care (MC) transaction flows include the following:

- Encounter data is sent to P1 by MCOs. This data is processed through P1 edit adjudication process to determine whether claims are allowable. Encounter data is subsequently sent to an actuary to calculate base premium rates for the MCO's.
- Rates (upload process)
- Adjustment factors (risk, age, gender, location) - These are adjustments made to the base rate. The adjustment factors are determined by the actuaries and entered in P1.
- Portal for clients to request change in MC plan.

## Client

For a client's claims to be paid through the P1 system, they must reside in the Client subsystem. Client data is entered in the Client subsystem through various sources including:

- DSHS's Automated Client Eligibility System (ACES)
- DSHS's Comprehensive Assessment Reporting Evaluation (CARE) system
- DOC's OMNI system
- Direct entry by HCA staff

## Provider

For a provider to be paid, providers must reside in the Provider subsystem. Provider data is entered in the Provider Subsystem through various sources including:

- OneHealthPort
- Agency Contracts Database (ACD)
- Enrolled providers can update certain information in the Provider Portal.
- Direct entry by HCA staff.

# State of Washington

CNSI contracts with LexisNexis contracts for provider integrity screening. P1 provider information is sent to LexisNexis. LexisNexis looks up provider data in multiple public data sources to verify/validate provider is able to provide Medicaid services and sends information back which is updated in the P1 system.

## Third Party Liability

Third Party Liability (TPL) refers to the legal obligation of third parties (for example, certain individuals, entities, insurers, or programs) to pay part or all of the expenditures for medical assistance under Medicaid. All other available third party resources must meet their legal obligation to pay claims before the Medicaid program pays for the care of an individual eligible. TPL information is communicated to HCA from various sources, such as client disclosure, claims, information obtained from the Support Enforcement Management System (SEMS) and outside vendors. TPL data is entered in ProviderOne including insurance company information, updating TPL invoices, and applying cash receipts to paid claims. TPL data is entered in ProviderOne through:

- Manual entry from Coordination of Benefits Unit
- SEMS interface

## **Rate Adjustment (Valuation)**

Fee-for-service and managed care premium payment rate factors are uploaded into ProviderOne. Ed Hicks' team is responsible for the fee-for-service rate uploads and Sam Trimble's, IT Business Analyst, area operates the managed care capitation rate factors.

For managed care, HCA pays a monthly premium rate to manage care organizations (MCOs) based on a rate per member per month (PMPM). There are about ten different rate templates for various medical and behavioral contracts as well as three rate templates for different foundational community support (FCS) contracts. There are five factors used to calculate the rates: base rate factor (BRF), age group factor (AGF), geographic region factor (GRF), risk adjust factor (ADF), and qualitative adjust factor (ADF). Pending on the managed care program they may use all or some of the rate factors. Ideally, HCA would like two months from the time a rate change is requested before it is uploaded and executed in ProviderOne. This time is required to adequately review changes, test for errors, receive proper approvals, and update ProviderOne. For fee-for-service, HCA directly pays providers for services rendered on qualified Medicaid members. The number of items to review is not as complicated as managed care so rate turnaround time is usually about 48 hours (target rate for quality control).

The rate change process begins with the System Operations and Implementation Unit (SOIU) receiving a rate update request via a ticket through a shared inbox and are triaged for assignment to Information Technology Specialist (ITS) staff within SOIU. Each ticket has a number that is used to track the progress of these requests. ITS staff first review the information provided to ensure it is complete. The review is only limited to data validation such as number formats and date ranges, etc. The ITS staff member then uploads the provided file into the ProviderOne User Acceptance Testing (UAT) environment. This allows them to verify that the file uploads appropriately before attempting to upload the file into production.

## State of Washington

ProviderOne has processing controls to help ensure the rate data uploaded is complete and valid. Updates that do not meet programmed edits will suspend to an error file that is reviewed by the ITS. If errors are identified, ITS staff notify the business area to make corrections and submit a new file attachment to the ticket.

Prior to uploading, Sam will also provide the business unit with a computed Rate Report for review. Once correct and successfully uploaded, ITS reviews the data and additionally compares the number of records in the source data to the number of records uploaded to ProviderOne. If everything processes appropriately, ITS then uploads the file into the production environment and the data goes through the same processing controls as in the UAT. When successfully uploaded, all rate updates will have an "In Review" status listed. ITS then updates and sends the ticket to Heidi DeVries, IT Specialist, who acts as an internal quality assurance for ProviderOne Operations (P1O). She reviews the rate data for accuracy and to ensure the requested changes conforms to medical related coding information which was provided to HCA from the Centers for Medicare and Medicaid Services (CMS).

HCA's vendor for ProviderOne, CNSI, obtains these types of files from the CMS website and then uploads them to ProviderOne. HCA will also upload reference data based upon decisions made by its own Policy Division. Heidi reviews all relevant information and determines whether to approve or reject the changes. Each rate's status reflects her decision. She then updates the ticket and sends it back to the ITS for closure, or closes the ticket herself.

Once approved, the system attaches dates to the rates data, including the effective date (when the rate was approved), the start date (when the new rate takes effect), and the end date. ProviderOne also has internal edits which will cause the claim calculation to fail out if data is invalid. After confirming the test runs produced correct results, P1O will push the rate changes to production **(Key Control #5 (manual), Rate upload review prior to production - Valuation)**.

### **How Transactions are Recorded in AFRS:**

Using the details included in a claim, system edits will verify eligibility and allowability of the claim based upon related information included in each of the above subsystems. This also allows the system to determine the type of claim. In this way, ProviderOne adjudicates all claims and assigns AFRS account codes to each transaction. When all the account codes are assigned, the Claims subsystem validates the assignment which includes checks for blank values, valid account codes, and AFRS table edits. As account code and table edits are updated in AFRS, there is an automated interface between AFRS and ProviderOne to update them in ProviderOne. If the transaction passes the edits in the subsystem, it is put into an Available for OFIN (Oracle Financials) status. OFIN stores general ledger, accounts payable, accounts receivable, and other financial information.

On a weekly basis, the Claims and Managed Care subsystems transactions are imported into the OFIN subsystem. It is within this subsystem that the Accounts Payable and Accounts Receivable netting and other processes occur to prepare the financial portion of the transactions to be sent to AFRS in batches. Transactions are sent via interface to AFRS for payment. AFRS and OST issue payments and sends a Warrant Wrap file to ProviderOne where OFIN and the original transactions are updated with the Warrant/EFT Number and Paid Date.

## State of Washington

HCA Accounting staff perform daily reconciliation between ProviderOne Batch Reconciliation Report 1280 and the AFRS Batch Interface log to verify the batches sent from ProviderOne are received and processed in AFRS (**Key Control #6 P1 to AFRS Reconciliation, Completeness**). Payment will not be made unless hard edits in ProviderOne are satisfied for validity of the claim and the provider based on the information in ProviderOne.

Transactions other than Managed Care or Claim payments, are sent to AFRS daily. These daily files include PHIPP/ESI payments and cash applications in TPL and Drug Rebate.

### **DSHS**

DSHS primarily relies on HCA for **rights and obligations (see Automated controls #1-4)** and **valuation (Key Control #5)** as HCA is the owner of ProviderOne. DSHS fiscal staff perform a similar daily reconciliation (**Key Control #6 P1 to AFRS Reconciliation, Completeness**) between ProviderOne report 1280 and AFRS Batch Interface log reports to ensure that batches are sent from ProviderOne to AFRS in their entirety.

To track the reconciliation process, an Excel workbook is created at the beginning of the month to document this process daily. The reconciliation process begins with Jesrie Beane, Fiscal Analyst, accessing the ProviderOne system and running a ProviderOne batch reconciliation report (Financial Report #1280). The P1 batch report specifies agency, batch date, batch type, batch number, batch count (count of all batched transactions), and batch amount. The ProviderOne batch type is categorized as "AH" (ProviderOne warrant payment) or "AI" (ProviderOne warrant cancellation).

Jesrie will take a screen shot of this report and paste it into the Excel workbook noted above with a new worksheet for each day of the month. The Fiscal Analyst then accesses the AFRS - Batch Interface (BI) system and then runs an AFRS batch interface report. The AFRS batch report also specifies agency, batch type, batch number, batch count, and batch amount. The Fiscal Analyst will take a screen shot of this AFRS report and paste it to the same worksheet as the ProviderOne batch reconciliation report. The Fiscal Analyst verifies on the AFRS batch report that the batch date, batch number, batch count, and batch amount shown in the AFRS report matches to the ProviderOne batch report. If the batch item on both reports match, the Fiscal Analyst will electronically sign the top of the worksheet where it says "Reviewer" for this batch date.

If there is a discrepancy between the two reports, Jesrie will send a copy of the worksheet with the two compared reports to Cheri Gullekson, Medicaid Accounting Manager, or Tanya Daymon, Fiscal Analyst 3, at HCA to resolve the issue. Documentation of the communication and resolution is also stored on the tab for the daily reconciliation.

### **Key Controls are as Follows:**

- Key Control #1 (Automated): ProviderOne verifies that the provider is eligible to provide the specific service covered by the plan to the specific Beneficiary. (**Rights and Obligations**)

## State of Washington

- Key Control #2 (Automated): ProviderOne verifies that the Beneficiary was eligible for the service at the time it was rendered. **(Rights & Obligations)**
- Key Control #3 (Automated): ProviderOne only pays up to the maximum claim procedure amount. If the claim's requested amount is less than the maximum amount, the requested amount is paid. **(Valuation)**
- Key Control #4 (Automated): ProviderOne verifies all procedure codes are within the valid HIPAA Transactions and Code Sets (TCS) and are covered by the State Plan. **(Rights & Obligations)**
- Key Control #5 (Manual): Health Care Authority reviews and approves the input of fee schedules into ProviderOne prior to being available for payment in processing in the system **(Valuation)**
- Key Control #6 (Manual): Fiscal analysts at both HCA and DSHS perform a daily reconciliation of amounts for batch interface uploads between the ProviderOne system and AFRS for AH (Payments and adjustments) and AI (Warrant cancelations or reissuances) batches **(Completeness)**

### Noted Weaknesses are as Follows:

HCA confirms that general controls are in place at CNSI by requiring a biennial Statement on Standards for Attestation Engagements (SSAE) No. 16 Type II audit to occur at the vendor, which occurs on even fiscal years in a biennium. During FY24, the Authority had 6 months of coverage for the SOC report. See audit issue at: [\[V: HCA Confidential IT Controls SOC Audit \(Part of ML\)\]](#). To support this finding, IT Audit identified the total dollars and number of records included in the ProviderOne data for all state and federal programs (see queries at [ProviderOne Summary Totals Queries](#)). Total dollars included in the data are **\$18,011,679,805.59** and total transactions are **140,740,691**.

**Additional testing will be preformed to determine if the general controls are sufficient, see [\[Key Controls #1 - 4 Edit Checks \(Automated\)\]](#).**

### D.4.PRG - Human Services

*Procedure Step:* Key Controls #1 - 4 Edit Checks (Automated)

*Prepared By:* DRR, 11/26/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To determine whether the following automated key controls for ProviderOne were in place and operating effectively:

## State of Washington

- Key Control #1: ProviderOne verifies that the provider is eligible to provide the specific service covered by the plan to the specific Beneficiary. (Rights and Obligations)
- Key Control #2: ProviderOne verifies that the Beneficiary was eligible for the particular category of service at the time it was rendered. (Rights & Obligations)
- Key Control #3: ProviderOne only pays the maximum claim procedure amount. If the claim's requested amount is less than the maximum amount, the requested amount is paid. (Valuation)
- Key Control #4: ProviderOne verifies that all coded data items consisting of procedure codes are within the valid HIPAA Transactions and Code Sets (TCS) and are covered by the State Plan. (Rights & Obligations)

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control was in place and operating effectively at the time of our testing. IT General controls related to the automated controls were adequate to ensure that the control operated consistently for six months of the audit period. However, we were unable to evaluate whether related IT general controls were adequate to ensure that the control operated consistently for six months of the audit period. See IT General Control understanding and testing at [IT General Controls](#).

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [Risk Assessment](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step.

Auditors should consider the following aspects of the automated control when gaining an understanding:

- Is there written documentation of the edit check?

*We would expect written system documentation that defines the edit check, including any formulas or logic or sources for comparison.*

- What transactions or data is subject to the edit check? How is the edit check triggered?
- What happens if the edit check is not passed?

*For example, some edit checks result in automatic rejection of a transaction or inability to post or proceed with a transaction. Other edit checks may flag a transaction for additional review or additional steps.*

# State of Washington

*Other edit checks may only result in a warning to the user, which the user could choose to ignore – in which case this would not normally be strong enough to be identified as a key control.*

- Is there any exception situations where the edit check can be by-passed or manually cleared or waived? If so, does edit check waiving or clearing generate any notifications, logs or exception reports? Also, what are procedures to review and follow up as needed on exceptions?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control.

To test the automated control, consider the following procedures:

- Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

- Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

Guidance/Criteria.:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**  
**[Information Technology](#) Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

Record of Work Done.:

## **STEP 1: Understand Automated Key Control**

The following automated key controls were identified:

# State of Washington

- Key Control #1 (Automated): ProviderOne verifies that the provider is eligible to provide the specific service covered by the plan to the specific Beneficiary. **(Rights and Obligations)**
- Key Control #2 (Automated): ProviderOne verifies that the Beneficiary was eligible for the service at the time it was rendered. **(Rights & Obligations)**
- Key Control #3 (Automated): ProviderOne only pays up to the maximum claim procedure amount. If the claim's requested amount is less than the maximum amount, the requested amount is paid. **(Valuation)**
- Key Control #4 (Automated): ProviderOne verifies all procedure codes are within the valid HIPAA Transactions and Code Sets (TCS) and are covered by the State Plan. **(Rights & Obligations)**

See Team FA control understanding at [Controls - ProviderOne](#).

On March 22<sup>nd</sup>, 2024, we met with Ed Hicks, IT System Admin, Angela Skinner, IT System Admin, and Kari Summerour, External Audit and Compliance Manager and Audit Liaison, to gain an understanding of the four automated controls over eligibility and allowability of claims. The automated controls cover **Provider and Beneficiary Eligibility, Payment Reasonableness, and Valid Codes**.

## Claims Background:

The ProviderOne (P1) system was created by Acentra (CNSI merged with Kepro and are now Acentra Health) who specializes in health information technology enterprise solutions. P1 adjudicates all claims and MCO encounters in the Claims subsystem. There are 120 data elements from a claim (also known as claim attributes or Domains) that are available to be used in the assignment process. Examples of attributes (or Domains) include Transaction Code Number (TCN), Claim Type, Procedure Code, Provider Enrollment Type, and Managed Care Transaction Type. Account coding has multiple elements: Agency, AFRS Program Code, Allocation Code, Appropriation Index, Fund, Organization Index, Program Index, Proj/SubProj/Phase, and SubObj/SubSubObj. Claims are identified by the Transaction Control Numbers (TCN) in ProviderOne. The tables containing the crosswalk between claim attributes and account coding reside in the P1 Reference subsystem. Using the details included in a claim, system edits will verify eligibility and allowability of the claim based upon related information included in P1 subsystems, such as Client, Provider, etc. Payment will not be made unless claims pass the hard edits. If a claim does not pass the hard edit, an error code will post on the claim indicating the reason it was suspended or denied. Each edit has a disposition when a claim is successfully validated of 'paid'. If a claim does trigger a validation edit, the validation edit is configured with a disposition either to 'suspend' or 'deny'. Claims that are suspended are reviewed manually by claims processing. Claims that are denied are automatically sent back to the provider unless in the rare instance the provider did not input any information that identifies them on the claim. In this case, the claim is denied and no action is taken. More details on this topic can be seen under Key Control #1 below.

## Overriding edits (Forcing edits)

- P1 allows for edits to be overridden. In the ProviderOne edit profile screen, each edit has a field named 'forcible' with a selection of 'yes' or 'no':
- If a claim edit forcible function is set to 'yes', this means that claims processing staff (adjudicators) can "force" the edit. There is guidance for adjudicating claims within P1 to help ensure claims are adjudicated correctly.



## State of Washington

- If a claim edit forcible function is set to 'no', claims processing staff cannot force the edit.

*Note: HCA has a process to override an edit, which occurs when a claim is NOT forcible but after research determines the edit should be **overridden** in a specific instance. In this case, the Systems Operation and Implementation Unit (SOIU), who configures edits, can switch the forcible field to 'yes' and push the claim through a triggered edit and determine the specific exception route the claim needs to follow. Further discussion regarding overriding edits through this process can be seen in the General IT section at [IT General Controls](#).*

See additional understanding of the automated controls in Team FA workpapers at: [Controls - ProviderOne](#).

### Important definitions:

- **Beneficiary:** The individual eligible for Medicaid benefits. Also referred to as the client. Beneficiary eligibility is determined by the Agency and Client Eligibility System (ACES) and the Comprehensive Assessment Reporting Evaluation (CARE) system managed and owned by the Department of Social and Health Services (DSHS). If eligible for care, the beneficiary will be covered by one of many health insurance providers that are Medicaid funded (for example Molina). Medicaid eligible enrollees that are receiving health care benefits.
- **Provider:** A licensed health care professional that provides services to beneficiaries.
- **Taxonomy:** Taxonomy codes are used to identify provider specialty/line of services. The Health Care Provider Taxonomy code set is a collection of unique alphanumeric codes, ten characters in length. The code set is structured into three distinct "levels" including Provider Grouping, Classification, and Area of Specialization. These classifications and designations detail the services providers can provide by procedure codes and modifiers to the Medicaid client. Providers may have multiple taxonomies. The taxonomy must be included in the claim. Taxonomies may be listed in multiple Benefit Service Plans.
- **Transaction Code Number:** The ProviderOne system assigns an 18-digit Transaction Control Number ([TCN](#)), also referred to as a claim number, to each claim received. When a claim is denied, the resubmission is considered a new claim and is assigned a new TCN. Suspended claims retain their original TCN. On all claims, the original and new TCN are available.
- **NPI:** A National Provider Identifier or NPI is a Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Standard. It is a unique, intelligence-free numeric identifier used to identify health care providers in standard transactions, such claims, eligibility inquiries and responses, claim status inquiries and responses, referrals, and remittance advices. *Note: If providers submit electronic files without a National Provider Identifier (NPI) and HCA doesn't know who to send them back to and they fall into what is known as "the black hole." The direct data entry system will not let a provider submit a file without an NPI, however, some providers choose to use their own software for billings and therefore submit electronic files. When electronic files are submitted, HCA doesn't control whether an NPI is input.*

### Key Control #1: ProviderOne verifies that the provider is eligible to provide the specific service covered by the plan to the specific Beneficiary. (Rights and Obligations)

As discussed above, the taxonomy code assigned to a provider determines the services the provider is eligible to provide. The Department of Health issues provider licenses. The license determines what taxonomy code numbers (services) the provider can provide. (For example:

## State of Washington

behaviorial specialists are not able to request payment for heart surgery based on their taxonomy.) ProviderOne verifies that the provider is eligible to provide the specific service requested for reimbursement based on their taxonomy. ProviderOne also compares the provided service to the beneficiary's Recipient Aid Category within the client's benefit service packages (BSP) and to the designated services that can be provided for the Taxonomy to determine whether the Provider can provide the service to that client. In addition, P1 will identify unallowed combinations of data such as an invalid taxonomy and modifier combination.

### **Key Control #2: ProviderOne verifies that the Beneficiary was eligible for the service at the time it was rendered. (Rights & Obligations)**

On May 20, 2024, we met with Lorena Delgado, IT System Admin, Ed Hicks, IT System Admin, and Kari Summerour, External Audit and Compliance Manager, and Audit Liaison to discuss key control #2.

Individuals are determined eligible for Medicaid primarily based on financial situation. Each eligible beneficiary is assigned to a 'RAC' (Recipient Aid Category) that designates what care they can receive. All RACs are assigned to a Benefit Service Plan (such as Take Charge Family Planning, Categorically needy). When a provider bills for a service, P1 will verify whether the service is covered under the beneficiary's plan. P1 also verifies beneficiary was eligible based on other factors, such as beneficiary is deceased, service was provided on a date that was before beneficiary was determined eligible for Medicaid or after eligibility ended.

### **Key Control #3: ProviderOne only pays up to the maximum claim procedure amount. If the claim's requested amount is less than the maximum amount, the requested amount is paid. (Valuation)**

If the claim is submitted that is at or above the allowed rate, the allowed amount will be paid. If the claim is less than the allowed rate, the claim amount will be paid.

There are instances where the allowed rate is overridden and manually priced. An example could be that a procedure wasn't priced as it should have been. When this occurs a help desk ticket is created approving the manually priced claims and an explanation is entered in the system.

### **Key Control #4: ProviderOne verifies all procedure codes are within the valid HIPAA Transactions and Code Sets (TCS) and are covered by the State Plan. (Rights & Obligations)**

The Center for Medicare and Medicaid Services (CMS) create the codes sets. The State Plan is the officially recognized statement describing the nature and scope of Washington State's Medicaid Program. Each state, through legislative and DHHS approval has state plan amendments they request to amend the state plan and potentially cover additional services. Approved services are detailed in State plan amendments for reimbursement purposes. ProviderOne compares all reimbursement claim's procedure codes to the configured HIPAA Transactions and Code Sets (TCS) to ensure procedures are allowed.

### **Summary of key automated controls**

## State of Washington

- Key Control #1: ProviderOne verifies that the provider is eligible to provide the specific service covered by the plan to the specific Beneficiary. (Rights and Obligations)
- Key Control #2: ProviderOne verifies that the Beneficiary was eligible for the service at the time it was rendered. (Rights & Obligations)
- Key Control #3: ProviderOne only pays up to the maximum claim procedure amount. If the claim's requested amount is less than the maximum amount, the requested amount is paid. (Valuation)
- Key Control #4: ProviderOne verifies all procedure codes are within the valid HIPAA Transactions and Code Sets (TCS) and are covered by the State Plan. (Rights & Obligations)

### **STEP 2: Confirm and Test Automated Key Control:**

See [Edit Selection Methodology Confidential](#) for edit selection methodology.

To gain a better understanding of the edit completeness monitoring controls in place, on 10/11/2024, Jon Howard, Team System Audit AAM, and Diana Evans, IT Auditor, met with the follow HCA staff:

Dineen Kilmer, P1 Section Manager

Ed Hicks, Systems

Angie Skinner,

Kari Summerour, Audit Liaison

There are several monitoring and control activities in place to help ensure the completeness and effectiveness of edits. The following is a summary of our discussion:

#### Collaboration and Expertise of Staff Requesting and Maintaining Edits

Edits are requested and monitored by different HCA Departments, such as Policy, Rates, Finance, etc., depending on the type of edit. Ed's group who create and maintain the edits similarly specialize by edit area to gain the extensive knowledge and expertise to maintain the edits and work with program staff. When creating or maintaining edits, updating rates, etc. Ed's SIOU staff work closely and communicate with the relevant program staff. We observed the communication between program staff and SIOU staff during our IT general control testing.

#### Daily Monitoring reports

Dineen informed us that the ProviderOne system automatically provides a daily Internal Daily Operational Dashboard report to both the Acentra operations staff and HCA regarding the previous day's adjudication and processing results. This report is used by HCA and Acentra staff to determine whether edits are functioning as intended. These reports provide indicators that processing is completed successfully and the results are within normal operating parameters. We observed the daily monitoring reports include suspended, denied, and paid claim percentages by source. See [DailyDashboardReport client](#) for example of the report.

## State of Washington

We inquired how staff are using the reports to determine whether edits are functioning as expected. Dineen stated that the monitoring reports are a job status report and they typically expect a paid/denied ratio of about 80/20. If the ratio is off for only a day, Dineen will not follow-up, however, if the ratio is off persistently for several days, she will follow up with Acentra. Acentra will provide a report of the top 10 edits that were posted during the time frame that HCA requests. Dineen will work with the System Administrators and look for irregular patterns of a specific edit paid/denied ratio to identify the root cause of the issue. Once they identify the edit(s) that are denying more claims, the System Administrator team will investigate and make the correction needed. Ed stated that he is looking for spikes up or down in the edit hitting. If he notices a spike in either direction, his group would research to determine whether an edit is not functioning properly.

We received a copy of the email that was sent 10/10/2024 and confirmed that 17 HCA staff received the email including Dineen, Ed, Angie, Jerry Britcher, Chief Information Officer, Todd Emans, P1 Operations Senior Manager, Michelle Osborne, P1 Operations Business Analyst, and Rebecca Carrell, Deputy Assistant Director, Medicaid Program Division, as well as four Teams/Groups at Acentra.

### Program Integrity

In addition to general IT controls, the Program Integrity group looks across claim history and compares amounts paid for services to policies and looks for overpayments. If an overpayment is identified, the funds will be recouped. Program Integrity consults with the System Administrators on an as needed basis if edits were causing overpayments. During an update meeting, we communicated the activity of program integrity to Team FA. Team FA will determine if they will gain any additional information related to Program Integrity.

### Provider Notification

Ed also mentioned that if providers were paid incorrectly, the provider usually notifies HCA quickly as they do not want to be underpaid and if they were overpaid, HCA recoups overpayments.

Based on inquiry and observations during our testing of edit changes and rate updates at Edit configuration and rate change testing confidential we determined that HCA has controls to monitor completeness and accuracy of edits. We did not perform further testing at this time. We determined the risk is low that missing (incomplete) edits would be significant to the ACFR.

**Testing:** We performed Rules Engine Testing and Edit Scenario Testing to test automated controls.

### Rules Engine Testing

P1 edits are performed through a series of rules. These rules are added and updated through a subsystem called the Rules Engine. HCA and Acentra developers use the RuleIT Composer component of RuleIT product to develop the rules. The RuleIT Composer compiles the rules and stores them in the database. The TraceTool contains descriptions in plain talk of what would cause the edit to post.

On May 17th, 2024, we met with Ed Hicks, IT System Admin, Angela Skinner, IT System Admin, and Kari Summerour, External Audit Liaison and Compliance Manager, to perform our rules engine testing. Prior to our meetings, Ed sent us the TraceTool information for each edit which

## State of Washington

described in plain talk what would cause the edit to post. Due to the rules engine having proprietary information within, Ed mentioned the vendor does not want to release this information and therefore Ed requested that we do not take screen prints.

- **Testing:** During our meeting, Angela presented her screen and we viewed the logic code in RuleIt for each error code selected. We compared the provided TraceTool information to the RuleIt code or configuration settings within the ProviderOne system and saw that either the RuleIt included code covering each item described in the TraceTool logic or it was covered by a ProviderOne configuration setting. See "Rules Engine Testing 2024" Tab here: [Edit population, selection and testing client confidential](#). During testing, Angela mentioned that there are times that notes within the rule engine in green font and could indicate if the edit needed to be updated. Being mindful of this, we reviewed the green font notes during each rule engine test to ensure no selected edits needed updated. We also inquired with Angela whether each edit's Rule Engine logic was current or if the edit's Rule Engine logic needed updated.
- **Results:** Of the 20 selections reviewed, 19 selections edit logic from TraceTool for the edit type agreed to the programming in the RuleIT rules engine and were current and did not need any updates. For one of the 20 selections, during testing, we were informed that edit 2255 was actually a configuration created many years ago by a former employee of HCA's and since it was not created correctly, it was never used. Edit 2255 is not a valid edit and should be identified as such within population of edits. We verified in ProviderOne that edit 2255 was not active. We removed this edit from our testing selections leaving us with 19 edits to test. While this does reduce our testing by one selection, we determined we still have an adequate amount of edits to test along with the work our Data Analysis team is performing. Ed informed us that the edit didn't have a zero in front and so it didn't match their error codes categories. With that, we reviewed the error code population again to determine if there were more edits without a zero. There was one, edit 2190, which was listed as obsolete. We searched for Obsolete edits and noted there were 191 obsolete edits in total. We followed up with Ed and asked why obsolete edits were still in ProviderOne. Ed stated that they were retained for auditing purposes. Kari informed us that Dineen Kilmer, IT Section Manager, stated that these edits take a substantial amount of work to develop and so they don't delete them in the case it could be used as a reference when creating new edits. There are also rare instances where an edit will have been removed and then implemented again in a later year. We inquired if all obsolete edits were set as inactive. Ed mentioned that he would need to look in ProviderOne to determine if obsolete edits are active. We inquired and were informed there is no review of obsolete edits. We also inquired if obsolete edits ever suspended or denied claims and showed up in the daily monitoring reports as being frequently triggered and Ed mentioned that he wasn't aware of an instance where they ever needed to force a real claim through an obsolete edit. Ed reviewed a few edits quickly during our meeting and mentioned that they were all set to inactive. I requested that Ed share his screen and we randomly selected obsolete edit 12965. We then verified the disposition was set to 'ignore' or inactive. We further inquired and were informed that because obsolete edits have inactive dispositions, the end dates being indefinite do not matter. Based on our understanding, obsolete errors are kept for a business purpose and are inactive. **No exception.**
- We were also informed that edit 09025 is currently posting because the system has already calculated an Allowed Amount for the claim based on loaded rates or Crossover payment methodology but the calculated Allowed Amount is higher than what Rates unit instructed SOIU to enter into the system as the high end for the posting logic. Per Ed, "These Suspend with Claims Processing and are sent to the

## State of Washington

SOIU unit to analyze per the error code text file based on the Claim Type. The Systems Operation Implementation Unit then reviews to see why this is posting. Normally it is a Medicare Crossover claim that has a very large Allowed Amount because of the severity of the care needed. If it is a Crossover and it looks correct we would force it through. Other issues our Rates department gets involved to verify if it is correct and can be forced and have the dollar amounts that cause the edit to post updated if needed." On June 6, 2024, we discussed this issue with Joel Todd, IT Auditor who performs the data analysis to further test P1 edits. Joel mentioned that his review does include reviewing claim over payments where the rate has been reduced, however, his review only covered paid claims, and does not include claim under payments where the claim was suspended/denied due to the maximum amount needing increased. We do not consider this to be an exception because the claims are suspended and adjudicated to ensure correct payment amount is made.

### Edit Scenario Testing

To conduct Edit Scenario testing, meetings were held on May, 20, 24, and 31, 2024 with Brandon Diltz, IT System Administrator, Ed Hicks, IT System Administrator, Angela Skinner, IT System Administrator, Lorena Delgado, IT System Administrator, and Kari Summerour, External Audit and Compliance Manager.

All tests were conducted in the test environment using real claims. The testing database contains the prior years claims and is brought in at the end of each year. Ed informed us that because all security patches are tested in the test environment prior to being loaded into production, he believes that the test environment does have the same security posture as the live environment. Ed also mentioned that there are much fewer users in the test environment. Note: Lorena performed the scenario test for Edit 00545 only because she is more familiar with Provider portals. Brandon performed the other 18 out of 19 scenario tests because he is more familiar with the validation edits and claims processing. To identify claims to test, Ed looked across the current data set of claims in the test environment for claims that had the error codes selected posted. For error codes that were not identified as already posting on claims, Ed identified claims that could be modified to trigger the error.

- Testing(Edit population, selection and testing client confidential) Edit Scenario Testing 2024): During each of our meetings, Brandon shared his screen and walked us through the scenario test for each edit error code to trigger. **Note: Transaction Code Number:** The ProviderOne system assigns an 18-digit Transaction Control Number (TCN), also referred to as a claim number, to each claim received. When a claim is denied, the resubmission is considered a new claim and is assigned a new TCN. Suspended claims' TCNs do not change.
- **Results:** During scenario testing, all error codes either activated when the claim testing scenario triggered the validation edit, or deactivated when the issue that triggered the error code was resolved. We did not identify any automated control deficiencies during edit scenario testing.

### Additional Data Analysis Testing (Documented by and Reviewed by Team DA staff):

We also determined we would complete some in-house CAATs (computer assisted audit techniques) work, which will allow us to look at the actual payments made during the audit period, and determine if ProviderOne processed payments as expected based upon our understanding. This will be a re-performance of the controls on a large scale, which will provide us with much more assurance if the controls are working as described.

## State of Washington

Additionally, since we are reviewing actual payments, we consider this dual purpose testing as it will provide us with a great deal of substantive evidence as well. This is in addition to the more detailed substantive work to be completed by the ACFR team. If any particular exceptions are identified during our testing, we will inform the line team so they can increase the sample size of their substantive work.

To complete our testing, we began by analyzing the population to determine what our testing population should include [see [FY24 Dual Purpose Procedure Code Testing](#)]. Based on this analysis, we determined we would consider all FY24 paid claims paid at the service line level. We then summarized this population by procedure code and claim type in order to identify specific procedure codes for testing [see [FY24 Dual Purpose Procedure Code Testing](#)]. Not all payments made through ProviderOne contain a procedure code, but we will concentrate on the population that does based upon the key controls identified. In order to get as much coverage of dollars spent during FY24 as we can, we initially determined we would select all procedure codes with more than \$3 million in paid claims for testing, which were not tested in our prior year reviews between FY14 and FY23. We would also exclude the OPPS claim type (testing OPPS claims requires more information than what is available in the ProviderOne data) from our selections. Following this criteria, we identified a minimal number of new codes to test, so we expanded our selection to include additional codes not tested since FY17 and FY18 [see [FY24 Dual Purpose Procedure Code Testing](#)]. This provided us with 10 procedure codes for testing, which included \$83,761,913.91 related to 833,438 claims [see [FY24 Dual Purpose Procedure Code Testing](#)]. This makes up 1.24% of the total population. Each year we try to focus on codes that have not been tested before in order to test as many codes as possible over the years of testing. Our queries to analyze and create the testing population for the procedure code testing can be seen at [[ProcedureCode Population Queries](#)].

The following provides the details of our data analysis testing as related to key controls #3 and #4:

**Key Control #3:** ProviderOne only pays up to the maximum claim procedure amount. If the claim's requested amount is less than the maximum amount, the requested amount is paid. **(Valuation)**

Based on our selection of procedure codes as described above, we identified the approved rates based on HCA and DSHS fee schedules available on their websites. We then analyzed associated medical and social service claims from the ProviderOne system and compared the paid amounts to these rates to ensure claims were paid at the appropriate amounts. We performed the testing with SQL queries [see [FY24 ProcedureCode Testing Queries](#)] and documented the results at [[FY24 Dual Purpose Procedure Code Testing](#)] (the testing of each procedure code is included in the last 10 tabs of the spreadsheet after the "Testing PSC" tab). Records tested included \$83,761,913.91 from 833,438 paid claims, which makes up 1.24% of the population of FY24 ProviderOne claims paid at the service line level with procedure codes [see [FY24 Dual Purpose Procedure Code Testing](#)]. The service line level payments with procedure codes make up over 81% of the total population of dollars paid in ProviderOne and over 89% of all records [see [FY24 Dual Purpose Procedure Code Testing](#)].

For the procedure codes included in our testing, we have determined the ProviderOne system is paying claims at or below the appropriate rates included in the identified fee schedules and reports. No exceptions identified.

**Key Control #4:** ProviderOne verifies all procedure codes are within the valid HIPAA Transactions and Code Sets (TCS) and are covered by the

# State of Washington

## State Plan. (Rights & Obligations)

During our testing of procedure codes [see [FY24 Dual Purpose Procedure Code Testing](#)], we found all procedure codes tested were part of the agency's plan for covered procedures. We did this by identifying each selected procedure code in its corresponding provider billing guide and fee schedules available publicly on the HCA and DSHS websites. We saw no evidence of claims paid through the ProviderOne system for services not covered by the agency. No exceptions noted.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control was in place and operating effectively.

## D.4.PRG - Human Services

*Procedure Step:* IT General Controls

*Prepared By:* DLE, 10/17/2024

*Reviewed By:* SHW, 11/7/2024

Purpose/Conclusion.

**Purpose:** To determine whether IT general controls related to the claims edits were in place and adequately designed to ensure the edits operated consistently during the audit period.

### **Conclusion:**

General controls related to the automated controls were adequate to ensure that the control operated consistently for six months of the audit period.

**We identified the following weaknesses related to the Acentra Health, LLC Provider One System and Organization Controls (SOC) 2 Type 2 audit:**

V: HCA Confidential IT Controls SOC Audit (Part of ML)

- The ProviderOne vendor's SOC 2 Type 2 audit did not cover the entire fiscal year 2024. The audit did not include the first six months of the fiscal year, July 1, 2023 - December 31, 2023.
- The Authority receives and reviews the Acentra Health ProviderOne SOC 2 Type 2 audit report to determine whether there are exceptions that require corrective action. However, there are no documented procedures for receiving and reviewing the report to ensure the review is adequately and consistently performed.
- The Authority did not maintain documentation to support there was a review of the SOC 2 Type 2 audit report.



# State of Washington

In addition, we noted the following insignificant weaknesses:

We identified the following weaknesses related to the process of forcing edits through the override process:

- Separation of duties between changing edits to forcible and forcing claims through edits was not system enforced. (Weakness #2) E: HCA ProviderOne Override IT Controls Confidential
  - The Authority did not have a monitoring process in place to ensure that all claims that were forced through the override process were authorized. (Weakness #2) E: HCA ProviderOne Override IT Controls Confidential
- There were no documented procedures for performing rate changes in ProviderOne. (Weakness #3) E: HCA Non-Confidential Provider One IT Controls

We noted no material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses.

- Who or what initiates program changes? (i.e. users, changes in legislation, special projects due to unexpected emergencies)
- Are changes requested in writing?
- How are program changes assigned to programming staff?
- Are changes to the program documented? How?
- Are there controls in place to ensure change requests are documented, authorized and appropriately assigned?
- Changes should be made in a development/test environment. Are changes adequately tested in a test environment before they are put into production? Who tests? Is the testing documented?
- What version control software is used?
- Does the version control software adequately control access to code, and provide for separation of duties between programmers, approvers, testers, and those moving code into production?
- Are there controls to prohibit multiple copies of the same program from being checked out at the same time?
- Could a programmer make unauthorized changes and put a program back into production without anyone knowing? What prevents them from doing so?
- Is the approval of an independent individual required before the program change is moved into production?

## **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

# State of Washington

## **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW.

Auditors should list and test each key program change control identified in the related "Gain an Understanding" step.

If tests are performed in a test environment, the auditor should ensure that the test environment has the same patch management controls as the live environment. If tests are performed in the live environment, the entity should be able to identify and correct any errors caused.

## **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

- [Instructions](#) are located in Team IT Audit's System's Sharepoint page.
- Details of IT Security related issues should NOT be included in any emails or helpdesks.
- Exit, ML and Findings should be separately communicated in an IT Security Results Document.
- Findings will be referenced, but not included in the audit report.
- All IT security-related recommendations must be reviewed by [Team IT Audit](#).
- Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

Record of Work Done:

# State of Washington

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

Redactions are highlighted in light orange.

## **STEP 3: Understand General IT Controls**

On April 15<sup>th</sup>, 2024, we met with the following people to discuss General IT Controls that provide assurance over the continued operation of the claim edit checks:

- Ed Hicks, IT System Administrator- Automated controls
- Angela Skinner, IT System Administrator- Configuration and Change Management
- Dineen Kilmer, IT Section Manager- SOC Audit review and vendor monitoring
- Heidi DeVries, IT Quality Assurance
- Samantha Zimmerman, Internal Controls Officer
- Kari Summerour, External Audit and Compliance Manager

Edits and rates must be programmed and updated correctly in order to rely on edits to consistently work as intended and providers to be paid the correct amount. Therefore, we determined program integrity and change management as the key control area for the automated controls identified at Key Controls #1 - 4 Edit Checks (Automated). Both the Acentra vendor and HCA are involved in the development and maintenance of edits as discussed below.

### **Vendor Controls:**

The ProviderOne system was created by Acentra (CNSI merged with Kepro and are now Acentra Health) who specializes in health information technology enterprise solutions. While HCA controls much of the day-to-day operation of the system, Acentra hosts the application and performs change management over the core P1 system. Therefore, processing integrity and change controls at Acentra are key general controls over the automated controls. HCA confirms that general controls are in place at Acentra by requiring in the contract with Acentra that a biennial Service Organization Controls (SOC) 2 Type 2 audit is conducted. In a SOC 2 Type 2 Audit, vendor controls are reviewed for security, availability, processing integrity, confidentiality, and privacy. These categories cover processing integrity and change management; therefore, the SOC audit addresses the IT general control areas applicable to our audit of automated controls.

**The ProviderOne vendor's SOC 2 Type 2 audit did not cover the entire fiscal year 2024. The audit did not include the first six months of the fiscal year, July 1, 2023 - December 31, 2023. (Weakness #1)** See V: HCA Confidential IT Controls SOC Audit (Part of ML). The previous SOC audit for P1 had an audit period of January 1 - June 30, 2022. The results of our FY22 review of the 6-month SOC report did not identify any issues. The following was taken from the S1Washington-FS22 TeamMate project: *The review covered a **six month period**, January 1, 2022 through June 30, 2022 and included expected review areas such as policies, procedures, system monitoring, access controls, network security, data center security, disaster recovery, among others. There were no exceptions noted. One area noted there had been no testing performed over the back up and recovery testing as it had not occurred within the audit time frame, and there was no mention of*

## State of Washington

*when the last testing had occurred. It was the opinion of the auditors that controls at CNSI related to the ProviderOne system operated effectively throughout the six month audit period. TA*

Dineen Kilmer, P1 Section Manager, receives and reviews the report to determine whether there are exceptions that require corrective action. Dineen explained that she reviews for findings and exceptions and will follow up with Acentra regarding a corrective action plan. Dineen further explained that Acentra submits an annual plan each year that includes items such as: user access, firewall (up-to-date), software upgrades, network upgrades, server upgrades, process improvements, and quality measures - keeping rework rates of UAT below 3%. This includes the submission of a monthly report where corrective action plans are tracked. Per Dineen, the vendor and HCA work together to determine the amount of time the corrective action will take. If Acentra did not correct deficiencies, there are consequences that could be enforced within the contract. Dineen stated that if this ever happened, she would work closely with HCA lawyers, but they have never needed to do so. Dineen provided us with a copy of the annual plan titled "Annual Plan for State of Washington ProviderOne System" dated 7/12/2023 which was during FY2024. *Note: Per the plan, this is not a contract requirement, rather an agreement between HCA and Acentra that this is a beneficial document for both parties.* We observed that the plan included the following areas:

- Major Activities Planned
- ProviderOne Software Releases
- System Maintenance and Infrastructure Activities
- Business and System Improvement Objectives
- Customer Service Performance
- Corrective Action

These areas align with the areas described by Dineen.

Dineen also provided us with the a montly progress report during the FY2024 audit period (November 2023). We observed that the monthly plan contains the same sections at the annual plan. As it relates to our automated controls, we noted the following from the document:

- 3.1.2 Other Contract Activities: Disaster Recovery Testing was performed on 9/14/2023. This was unknown based on our review of the SOC report.
- 4 Releases and release schedules
- 5.1 Change Requests

Based on our observations, an annual plan and monthly progress reports are submitted to HCA that communicate changes and corrective action plans.

Per Dineen, there are no formal procedures for receiving and reviewing the SOC audit report to ensure review occurs and is performed consistently. **The P1 Section Manager, receives and reviews the Acentra Health ProviderOne SOC 2 Type 2 audit report to determine whether there are exceptions that require corrective action. However, there are no documented procedures for**

# State of Washington

**receiving and reviewing the report. (Weakness #1)** See V: HCA Confidential IT Controls SOC Audit (Part of ML)

**Key General IT Control #1- The ProviderOne IT Section Manager, reviews the SOC Audit Report to determine if there are any findings that require corrective action to be taken. If corrective action is required, the ProviderOne IT Section Manager will monitor the corrective actions taken by reviewing the submission of the vendor's monthly report to HCA.**

## **HCA Controls:**

In addition to vendor controls, user entities (HCA) must also have controls over processing integrity and change management. We identified the following general controls that provide assurance over the complete and accurate operation of the claim edit checks:

- User Access
  - Access to turn the "force edit" function on/off (in other words, override the edit)
- Change Management
  - SOC Audit report review and vendor monitoring- Acentra
  - Configuration Management
    - Edit Configuration and Changes
    - Simple Rate Changes (Valuation) Note: We selected simple rate changes because they apply to Key Control #3: *ProviderOne only pays up to the maximum claim procedure amount. If the claim's requested amount is less than the maximum amount, the requested amount is paid.* (Valuation).
    - General Charge Modes
- Daily Monitoring Reports
- Program Integrity

## **User Access**

Each edit has a field named 'forcible' with a selection of 'yes' or 'no' which can be viewed on the P1 edit profile screen. If a claim edit forcible function is set to 'yes', this means that the claims processing team can force the claim through the edit. Based on our automated control testing population, there are currently 1,866 total edits. There are currently 1,645 edits that are forcible by claims processing. Each of these forcible edits has an exception path to follow. Every error code that could be forced by claims processing has a unique text file attached that gives instructions on how to force the specific edit. Additional information related to forcing edits is located on page 3: Error Code Maintenance\_client\_confidential.

If an edit's forcible function is set to 'no' then the claims processing team (adjudicators) can not force the claim. Currently, there are 221 edits that cannot be forced through the regular adjudication process. Because of their level of expertise related to edits and associated exception paths, only designated HCA Enterprise Technology (ETS) staff can switch the forcible field to 'yes', thereby overriding the edit. **Access to change an edit to be forcible (Override) is restricted to only those individuals who need access to perform their job duties. (Key**

## State of Washington

**General IT Control #2)** Occasionally, there is a request from the Clinical Policy group to override an edit due to a specific business need. Clinical Policy group is a group of clinicians, nurses, and doctors that are hired to perform review of claims submitted. Once the edit is made forcible and the claim is forced through by the ETS group, the edit's forcible field will then immediately be changed back to 'no' to prevent claim processing adjudicators from erroneously forcing other claims through the edit. The claim history and the edit history both record any edits that were changed or forced through.

### **Manual overriding edits - Significance**

There is a report (10377) that details forced claims, however, this report includes the edits that are determined to be set to forcible (not an override); therefore, this report would include all edits that were forced through the regular adjudication process. We are unable to use this report to determine materiality because it does not identify which edits were overridden and then forced. Ed requested the vendor produce a report listing all the edits that had been overridden by Ed's SIOU group. Ed provided us with the report of claims that were manually overridden. There were two claims on the report, one for \$89.00 and the other for \$943.56. Ed provided an explanation for each claim that was overridden. The number of claims and amount of the claims overridden is insignificant to the ACFR. See [Manual override of edits\\_client](#)

HCA has not configured a usable query/report that details overridden claims nor do they monitor for unauthorized overrides. **HCA did not have a monitoring process in place to ensure that all claims that were forced through the override process were authorized. (Weakness #2)** E: HCA ProviderOne Override IT Controls Confidential

### **Change Management**

There are three change management areas that relate to our automated key controls: Edit configuration and change controls, Simple Rate changes, and General Charge Modes. Configurations all follow a process that is enforced by system user profiles. Only specific users have the various role/profile to approve specific configuration changes in the Production environment.

#### 1. Edit configuration and change controls

Kari Summerour, HCA Audit Liaison, provided the following written procedures related to Error Code Maintenance; [Error Code Maintenance\\_client\\_confidential](#) that covers "adding a new error code" on page 8, the KT life cycle; [KT Lifecycle\\_client\\_confidential](#) that covers the System Development Life cycle on page 1, and KT Testing Process [KT Testing Process\\_client\\_confidential](#) that covers the User Acceptance testing on page 1. **Key General IT Control #3: New rule engine configurations go through a KT (change) process that includes user acceptance testing to ensure changes are authorized, tested, and function as intended.** Configurations requests come from the Policy group at HCA. The rate change process begins with the System Operations and Implementation Unit (SOIU) receiving a rate update request via a ticket through a shared inbox and are triaged for assignment to Information Technology Specialist (ITS) staff within SOIU. Each ticket has a number that is used to track the progress of these requests. ITS staff first review the information provided to ensure it is complete. The Policy group or Finance will submit a KT request form and Jira ticket including their proposed change to the IT Systems team for review. The Jira ticketing system is used by both HCA and Acentra to communicate.

## State of Washington

Angela performs the initial review of the request for new configuration and identifies how the edit will be configured and adds it to an edit change release log. Angela is the only staff that creates logic. The logic will be created and added to the rules engine (RULEIT) during a KT meeting. All changes are made during a KT meeting which includes the ProviderOne users and a Quality Assurance person attending this meeting. Once the logic is added to the development area of the rules engine, the new edit logic is ready for the vendor to perform testing. Acentra, the vendor does system integrity testing and regression testing to check the overall health in the system.

Once Acentra performs testing, Acentra will load edits into an HCA testing environment and the HCA end user who requested the change will conduct user acceptance testing (UAT) by creating and processing new claims with scenarios to trigger the new rule. UAT, where corrections are communicated to the vendor, if necessary, typically lasts four weeks. Once all test cases have passed, Angela will inform the vendor.

After UAT, a regression testing deck is run to determine if there were any adverse effects of the change. Once regression testing is complete, the new edit is loaded into the live environment by Acentra. Only Acentra has access to the live environment. Angela stated that staff at HCA staff do not have access to upload changes to the rule engine into the live environment. Once the change is uploaded by Acentra, a live test is also conducted by HCA.

There are instances where after an edit is uploaded into the live environment, an increased number of claims are denied. In this event, staff will investigate to see what is wrong with the newly configured edit. We were informed that because edits are tested by HCA and the vendor it isn't often an edit makes into the live environment configured incorrectly.

Changes made to the rule engine are manually logged in the history of the rule that was changed. When a staff member checks out the rule for an update, the system requires a note before the change can be checked back in. The note can be any description that HCA inputs. *Note: HCA does not have access to the live environment to the rule engine, any changes made would be routed through the change control process described above.*

Most edit changes require the change to be made in the rule engine, however there are some that do not. For example, limit edits, conflicts, duplicates are configurable directly in ProviderOne. The edits that do not require the rule engine follow the same process as simple rate changes detailed below. Similar to simple rate changes detailed below, edits that are created within ProviderOne are created by the System Admin team, primarily Angela Skinner and reviewed by Quality Assurance, primarily Heidi Devries.

### 2. Simple Rate changes (Valuation)

Fee-for-service and managed care premium payment rate factors are uploaded into ProviderOne. Ed Hicks, IT System Admin team is responsible for the fee-for-service rate uploads and Sam Trimble, IT Business Analyst (BA) area operates the managed care capitation rate factors. We inquired with and were informed by Ed and Sam that there are no written procedures for rate changes. **There were no documented procedures for performing rate changes in ProviderOne. (Weakness #3)** See E: HCA\_Non-Confidential Provider One IT Controls

## State of Washington

For managed care, HCA pays a monthly premium rate to manage care organizations (MCOs) based on a rate per member per month (PMPM). There are about ten different rate templates for various medical and behavioral contracts as well as three rate templates for different foundational community support (FCS) contracts. There are five factors used to calculate the rates: base rate factor (BRF), age group factor (AGF), geographic region factor (GRF), risk adjust factor (ADF), and qualitative adjust factor (ADF). Depending on the managed care program they may use all or some of the rate factors. Ideally, HCA would like two months from the time a rate change is requested before it is uploaded and executed in ProviderOne. This time is required to adequately review changes, test for errors, receive proper approvals, and update ProviderOne. For fee-for-service, HCA directly pays providers for services rendered on qualified Medicaid members. The number of items to review is not as complicated as managed care so rate turnaround time is usually about 48 hours.

Files with new or redefined code sets (CMS HIPAA codes, American Medical Association Current Procedural Terminology (CPT) codes, and American Dental Association CPT codes) are sent to HCA from CMS quarterly via email. These are provided about two months prior to the new quarter starting. Within the file, there may be new services/codes, updated services/codes, or service/codes that are ending. The services and codes within the file are provided by Heidi to Clinical Policy to review and determine applicability and coverage and if they are within the State Plan Amendment. Once applicability and coverage are determined, Clinical Policy will request the rates to be configured by the P1 System Operations and Implementation Unit (SOIU) staff who will request the rates be loaded by the vendor Acentra. Acentra will load the rates into a testing environment for Quality Assurance review and approval. Rates are loaded into ProviderOne with effective dates for claims processing. Heidi verifies that the codes are input into ProviderOne accurately and also runs test claims to determine if the system is correctly referencing the codes.

Existing rate change process begins with the System Operations and Implementation Unit (SOIU) receiving a rate update request ticket through a shared inbox. The requests are triaged for assignment to Information Technology Specialist (ITS) staff within SOIU. Each ticket has a number that is used to track the progress of these requests. ITS staff first review the information provided to ensure it is complete. The review is only limited to data validation such as number formats and date ranges, etc. The ITS staff member requests Acentra upload the provided file into the ProviderOne User Acceptance Testing (UAT) environment. This allows them to verify that the file uploads appropriately before attempting to upload the file into production. ProviderOne has processing controls to help ensure the rate data uploaded is complete and valid. Updates that do not meet programmed edits will suspend to an error file that is reviewed by the ITS. If errors are identified, ITS staff notify the business area to make corrections and submit a new file attachment to the ticket. Prior to uploading, Sam (BA) will also provide the business unit with a computed Rate Report for review. Once correct and successfully uploaded, ITS reviews the data and additionally compares the number of records in the source data to the number of records uploaded to ProviderOne. If everything processes appropriately, ITS then uploads the file into the production environment and the data goes through the same processing controls as in the UAT. When successfully uploaded, all rate updates will have an "In Review" status listed. ITS then updates and sends the ticket to Heidi DeVries, IT Specialist, who acts as an internal quality assurance for ProviderOne Operations. She reviews the rate data for accuracy and to ensure the requested changes conforms to medical related coding information which was provided to HCA from the Centers for Medicare and Medicaid Services (CMS). Once Heidi determines rates are accurate and conforms, she approves the rates. The status of the rate updates change to "Approved" and are active in Production. Heidi then updates the ticket and sends it back to the ITS for closure, or closes the ticket herself. Vicki Sutton, IT Quality Assurance, is Heidi's backup and is authorized



## State of Washington

to approve rate changes and other QA related duties. **Key General IT Control #4: All simple rate changes are reviewed and approved by Quality Assurance prior to being implemented in production to ensure simple rate changes function as intended.**

### 3. General Charge Modes

General Charge Modes are rates that are configured behind the scenes of ProviderOne by the vendor in a back-end area that HCA does not have access to. General charge modes are developed and tested by Acentra (CNSI) and HCA prior to upload into production. General Charge modes are specific to how different types of claims can process. As an example, General Charge Mode 252 is used exclusively on Hospice pricing when the client lives in a county that HCA does not load the rates for that county. Ed was unaware why the system was set up to have the vendor load the General Charge Modes. He stated that this was the way the system was configured originally. Ed further stated that General Charge Modes are not changed as often as other rates. For example, HCA changed one earlier this year for hospice that hadn't been changed since 2006. Most General Charge Modes are changed every couple years.

To determine whether charge mode rate changes were significant for the FY2024 ACFR audit, we requested a list of all changes made during FY2024. Ed provided us with a list of all the charge mode rate changes along with the SQL logic for pulling the data at FY2024 Charge Mode Rate Changes Client. (P/C: To determine significance of the general charge modes rate changes) There were 49 total. There were 60,365 simple rate changes (see testing of Key Control #4 below for identification of population). Charge mode rate changes account for .08% of rates changes. Therefore, for the FY2024 ACFR audit, we determined that we will not test charge mode rate changes. We will test simple rate changes as they are the majority of rate changes that occurred during the year.

### **Summary of Key General IT controls**

Key General IT Control #1- The ProviderOne IT Section Manager, reviews the SOC Audit Report to determine if there are any findings that require corrective action to be taken. If corrective action is required, the ProviderOne IT Section Manager will monitor the corrective actions taken by reviewing the submission of the vendors monthly report to HCA.

Key General IT Control #2- Access to change an edit to be forcible (Override) is restricted to only those individuals who need access to perform their job duties.

Key General IT Control #3: New rule engine configurations go through a KT (change) process that includes user acceptance testing to ensure changes are authorized, tested, and function as intended.

Key General IT Control #4: All simple rate changes are reviewed and approved by Quality Assurance prior to being implemented in production to ensure simple rate changes function as intended.

### **STEP 4: Confirm Key General IT Controls**

See screen prints at Gen IT KC confirmation system documentation\_client\_confidential for confirmation work below.

**Key General IT Control #1- The ProviderOne Section Manager, reviews the SOC audit report to determine if there are any findings that require corrective action to be taken. If corrective action is required, the ProviderOne Section Manager will monitor**

## State of Washington

### **the corrective actions taken by reviewing the submission of the vendors monthly report to HCA.**

Because there were no corrective actions from the 2022 SOC audit that were still being monitored during SFY2024, and the 2024 SOC audit will not be received until August 2024, there is no activity during the audit period to walk through. Therefore, we will not confirm this key general IT control but rather it will be tested under Step 5 below.

### **Key General IT Control #2- Access to change an edit to be forcible (Override) is restricted to only those individuals who need access to perform their job duties.**

To confirm that only system administrators have access to override a claim, on May 7, 2024, we met with Ed Hicks, IT System Admin and Kari Summerour, External Audit Liaison to perform a walk through. Ed first logged in to the test environment as a claims processor [12] that had error code 02190 posted on it. As Ed was logged in as a claims processor, he then tried to resolve error code 02190 by forcing it. The system denied the user from forcing the claim through the edit, see screen prints #1 and #2. We noted there was a claim supervisor role and requested that Ed also log in as a claims supervisor (Role: OCP MAS 4 MAS 5) and attempt to force the claim through the edit. The system denied the claims supervisor from forcing the edit. After we observed the claims processor, and supervisor roles not allowing the user to force the claim, Ed logged in as a System Administrator [12]. Using this role, Ed changed 02190 to be forcible and demonstrated that he could resolve the edit posting and force the claim through the edit, see screen prints #3, #4, and #5. Screen print #3 shows that the edit was changed to be forcible. Screen print #4 shows that during the 4th cycle run of the claim, prior to the edit being changed to forcible, edit 02190 was denied. Screen print #5 shows that after the edit was changed to be forcible, error code 02190 no longer populated on the list of error codes. [12]

: HCA ProviderOne Override IT Controls Confidential [12]

### **Key General IT Control #3: Rule engine configurations go through a KT (change) process that includes user acceptance testing to ensure changes are authorized, tested, and function as intended.**

On June 4th, 2024, we met with Ed Hicks, IT System Administrator, Angela Skinner, IT System Administrator, and William Sogge, External Audit Liaison to walk through a recent new edit configuration and confirm change management controls are in place. Angela presented her screen and walked us through ticket# P10036010 that requested three new encounter- pay and report edits to be configured, see Screen print #12. These edits were identified as error code #s 05050, 05051, 05052. This request was submitted by Kasandra Wilson, Coordination of Benefits and Claims Processing Section Manager on August 17th, 2023. Pay and report edits are soft edits that report information from paid claims for tracking purposes. Pay and report edits do not suspend or deny claims from payment when triggered. Because we were using a historical configuration request, we requested that Angela share with us the system enforced process flow that was linked to the ticket. Angela shared the system enforced process flow, see Screen print #11. After we reviewed the ticket and system enforced process flow, we requested that Angela show us

## State of Washington

the plain talk logic that was requested from Kasandra that was attached to the ticket. Angela walked us through the logic for each edit, see Screen print #13. Angela then showed us that these change requests along with many other change requests were rolled up into one large change request 'KT for R1 2024'. Angela showed us in the ticketing system that KT for R1 2024 was developed and tested by Acentra and then moved back to HCA for User Acceptance testing, see Screen print #14. Angela then logged into the POTS User Acceptance Testing system and showed us that KT for R1 2024 including tests for new edits 05050, 05051, 05052 was tested by Heidi Devries, Quality Assurance, see Screen print #15. Angela then showed us in the ticket history that after Heidi completed UAT in POTS, Angela then went back into the ticket in ProviderOne and approved UAT, see Screen print #14. Acentra then resolved the ticket and Angela closed the ticket, see Screen print #14.

### **Key General IT Control #4: All simple rate changes are reviewed and approved by Quality Assurance prior to being implemented in production to ensure simple rate changes function as intended.**

On June 3, 2024, we met with Ed Hicks, IT System Administrator, Lorena Delgado, IT System Administrator, Angela Skinner, IT System Administrator, Heidi DeVries, IT Quality Assurance, and Kari Summerour, External Audit and Compliance Manager to walk through and confirm Key General IT Control #4.

Lorena shared her screen and began walking us through a recent rate change request (Ticket #P10062208) that was requested on May 29, 2024 by the Rate group (Kathryn Mesaros, Social Service Billing and Training Program Manager). This rate change request was to Update the rate for SA298 and edit logic for logic 30149. Because tickets sometime come with multiple requests within, this ticket also had an edit configuration update. Here, we will only focus on the rate change for SA298 which is a Procedure Rate. This specific procedure rate was being updated from \$0.01 to \$4,000 to \$0.01 to \$10,000 effective May 1, 2024.

Lorena reviewed the Excel file submitted with the ticket by the Rates group see Screen print #6 and the attached excel file containing the rate update at Screen print #7. All elements on the rate change request were accurate. Lorena then logged into ProviderOne and uploaded the rate sheet into UAT and ran ProviderOne's processing verification on the rate sheet. ProviderOne returned no errors. Lorena then logged in as an approver and approved testing. *Note: The rate does not go live until after the QA Review in the Production environment.* Once testing was complete and approved, Lorena logged in as a tester in the production environment and conducted the same process and uploaded the rate sheet into ProviderOne's processing verification, see Screen print #8. Lorena again ran the Processing verification on the rate sheet in production and when ProviderOne returned no errors, see Screen print #9, Lorena then approved the rate sheet testing in Production. Batch instance number 500105893 is for file review tracking purposes. Lorena showed us that she did not have the profile (Operations and Support System Approver) to approve rates in production. Once Lorena approved the rate sheet's testing in Production, she took a copy of the rate sheet loaded into production and uploaded it into the help desk and assigned the ticket to Heidi Devries, IT Quality Assurance. Heidi shared her screen and logged in with the profile Operations and Support System Approver and walked us through her review and approval. Heidi verifies that original ticket matches the approved ticket in Production and that no changes were made. Heidi also expanded the rate past two decimals and verified that the rate ends in all zeros. Heidi did not identify any necessary revisions and so she approved the rate and it was then active in ProviderOne including a definite start date of May 1, 2024 and a indefinite end date, see Screen print #10.

# State of Washington

## **STEP 5: Test Key General IT Controls**

Because the SOC audit only covers half of the audit period and only 6 out of 24 months in a biennium, in order to support a LOW control risk assessment, we need to determine if we could rely on other compensating General IT controls (Key General IT Controls #1, #2 #3, and #4), therefore, we tested General IT controls as detailed below.

**Key General IT Control #1 - The ProviderOne Section Manager, reviews the System and Organization Controls (SOC) report to determine if there are any findings that require corrective action to be taken. If corrective action is required, the ProviderOne Section Manager will monitor the corrective actions taken by reviewing the submission of the vendors monthly report to HCA.**

We received the Acentra SOC 2, Type 2 audit report from Kari Summerour, External Audit Liaison/Internal Auditor. A SOC 2, Type 2 audit reports on the controls at a service organization relevant to security, availability, and processing integrity, providing us assurance over IT general controls (including network security, user access controls, and physical security) of the ProviderOne system at Acentra Health (previously known as CNSI). Per Dineen Kilmer, ProviderOne Operations Manager, she reviewed the report to determine whether the report meets HCA's needs and whether controls are in place including if any exceptions were noted. Dineen stated she does not have any documentation to support her review of the SOC report covering our audit period. **The Authority performs a review of the System and Organization Controls audit report for the ProviderOne system at Acentra Health. However, there is no documentation retained to support the review occurred and what was included in the review. (Weakness #1)** V: HCA Confidential IT Controls SOC Audit (Part of ML)

Through observation of the report, we determined the audit was completed by UHY LLP, a licensed independent CPA firm that provides services nationally. The review covered a **six month period**, January 1, 2024 through June 30, 2024 and included expected review areas such as policies, procedures, system monitoring, access controls, network security, data center security, disaster recovery, among others. We reviewed the test results for the three applicable trust services (Category: Security, Availability, and Processing Integrity). There were no exceptions noted. The audit report stated that testing of the Business Continuity and Disaster Recovery (BCDR) plan could not be tested, because there was no BCDR testing during the audit period. There was no mention in the report of when the last BCDR testing had occurred. There also was no testing of incident response as there were no incidents that required remediation during the audit period. It was the opinion of the auditors that controls at Acentra Health related to the ProviderOne system operated effectively throughout the six month audit period.

Based upon our review of the completed audit report, we have assurance Acentra had appropriate general controls in place during the six month period included in the review. However, since the report only covers half of fiscal year 2024, we do not have assurance covering a majority of our audit period and we are unable to rely on the controls tested above for the entire period. Due to this, we cannot consider the prior year audit exception completely resolved.

**Key Control #2 - Access to change an edit to be forcible (Override) is restricted to only those individuals who need access to perform their job duties.**

## State of Washington

**Scenario:** Determine whether access to change an edit to be forcible is limited to only those individuals who need access to perform their job duties.

**Selection:**

Population: All users who have the ability to force claims through edits.

We met on May 15, 2024 with Lisa Hadley, Senior P1 Business Analyst, Ed Hicks, IT System Administrator- Manager, and Kari Summerour, External Audit and Compliance Manager to determine what roles and profiles allowed access to the edit forcibility function, and the users who were assigned those roles/profiles. Access to functionality is controlled by the ProviderOne page that the particular function is on. For example, the function to force edits is on page ID 'pgErrorCodeDetail(Claims)'. Each page (identified by page ID) is associated to various roles. Those roles are associated to profiles. The profiles are associated to users. It is the role/profile combination that allows access to the functions within each page.

There are two roles that combined with their respective four profiles provide access to force edits:

[12]

[REDACTED]

[12]

[REDACTED]

[12]

[REDACTED]

There were a total of 31 users with one of the combination of role/profile listed above. Some users were listed in two profiles and appear on the list twice.

**Testing:** To conduct testing, we met on May 30, 2024 with Lisa Hadley, Senior P1 Business Analyst, Ed Hicks, IT System Administrator- Manager, Kari Summerour, External Audit and Compliance Manager, and Jennifer Robinson, Application Development Manager. We observed security screens from P1 and recorded all users within each profile. For each user listed within the profiles identified, we inquired with ProviderOne leadership (Ed and Jennifer) if the user was an active HCA employee, and whether the user needed such access to conduct their daily job duties. We also compared the users listed to the Enterprise Technology Services (ETS)- ProviderOne Operations organization chart: [HCA ETS.org](https://www.hca.wa.gov/ets)

# State of Washington

[chart\\_client](#). Testing can be seen here: [User Access Testing\\_confidential](#) .

**Results:** Based on inquiry with ProviderOne leadership, we did not identify any user with access that should not have access. All users were current employees who still work on the ProviderOne system and either configure or test edits, are a leadership member, or acting as a backup. We identified one backup user, Dineen Kilmer who is the Section Manager for the System Operations and Implementation Unit who was identified as a back up only. Because there are many others who could act as a backup, we inquired if there were more reasons Dineen required such access or if it could be removed. We were informed that Dineen needs to retain access for 3 reasons: analyzing claims issues, as a backup when assistance is needed, and to have the ability to view the whole breadth of an issue to determine a solution. Dineen is also trusted as the person to investigate any internal or external frauds within the system. **No Exception.**

**Key General IT Control #3: New rule engine configurations go through a Knowledge Transfer (KT) change process that includes user acceptance testing to ensure changes are authorized, tested, and function as intended.**

**Population/selection:** We logged into ProviderOne via its web interface, clicked on the Claims subsystem tab, clicked the Administration link, and clicked the Error Codes. We then saved the list of error codes by selecting the 'save to XLS' function. There were 2,253 edits in total. We then filtered to edits that had 'Effective Date' within State Fiscal Year 2024. There were 82 new edits with an effective date starting during SFY2024. Using the sampling spreadsheet for small populations, we determined our sample size is 14. We then used the random number generator to select our sample.

## Testing:

We uploaded our sample into HCA MFT and requested that HCA submit screen prints of the change request ticket and the POTS User Acceptance System. For each selected error code we reviewed the ticket and POTS documentation to determine whether changes included user acceptance testing. When providing the documentation, Ed explained that *"Simple configuration changes are rarely tested as we have done them for over a decade now and we know how this works. If we have to move to the next level of system change that requires KT these are tested because this is new functionality that we haven't done before or is different than what we have done in the past. Sometimes simple configuration will be tested if it is very extensive, and we want to make sure we did everything correctly."* Ed also stated that text only changes are not tested. Based on Ed's response, we do not expect text only changes or simple configuration changes to be tested.

Out of the 14 edit changes we selected for testing, Ed provided the following additional information:

- Six were simple configuration changes and no KT user acceptance testing was determined necessary.
- Four were text file changes, there was no configuration change to test.
- Four changes were determined necessary to have testing through the KT process.

See testing matrix at [Edit configuration and rate change testing\\_confidential](#)

## State of Washington

### Summary of testing:

- *Six simple configuration changes where no KT user acceptance testing was determined necessary.* We reviewed the requests and observed there was communication between the requestor and the person who made the change to provide assurance simple configuration changes were made as requested. No further testing necessary.
- *Four text file changes, there was no change to test:* For each of these text change requests we verified through observation of the ticket that the request was only for changes to the text. The person assigned to the ticket communicated with the requestor regarding the text change and when it was complete. We confirmed through inquiry of Heidi that text only changes are not tested. No further testing necessary.
- *Four changes were determined necessary to have testing through the KT process.*  
For the four changes that were at a complexity level needing testing, we observed screen prints from POTS and verified that testing was documented for all four changes. No exceptions.

From our sample of 14 edit changes, only four were considered new or complex enough to be "new configurations" that go through the KT change process. We determined all four were tested. We did not pull more changes for testing as all four passed the control testing and we are not planning on relying on the automated control for substantive testing (Control Risk at Max) at Substantive Test. **No Exception.**

**Key General IT Control #4: All simple rate changes are reviewed and approved by Quality Assurance prior to being loaded into production to ensure simple rate changes function as intended.**

**(Note: This testing also used for manual KC#5 for Team FA at Key Control #5 (Manual))**

**Population:** We generated populations of rate upload files for both fee-for-service and managed care within ProviderOne by pulling the following exports:

#### **Fee For Service:**

Rate Settings -> Rate Group drop down:

- Provider Rates- 9,102 rate changes
- Program Rates- No rate changes
- Group Rates- 1 rate change
- Proc/Svc/Revenue Rates- 36,841 rate changes
- Client Rates- 12,326 rate changes
- Taxonomy Rates- 2,080 rate changes
- DRG Value Rates- No rate changes

Filter By: Upload Date **07/01/2023 to 06/30/2024** And: File Name **%** And Status: **Approved.**

# State of Washington

## Managed Care:

Managed Care -> PMPM Rate Configuration and Select View Summary Rate Report. Then use the Filter by drop down and select Generate Date and input **07/01/2023 to 06/30/2024**. There were 480 rate changes

The process of rate change review, approval, and upload are similar between the MC and FFS rates, but the requests originate from different teams. We combined all FFS and MC rate change files into a single population to draw our sample. There were 60,365 total rate changes. Because multiple rate changes are included in a ticket, we summarized our population by File Name, and Upload date. This results in 687 file names or tickets.

**Sample Selection:** There were 687 tickets for rate changes in total during state fiscal year 2024. Based upon the sample criteria (population quantity/amount, expected misstatement, tolerable misstatement, and level assurance) we determined a sample size of 59 for each testing population. We will be using the same testing criteria for the FY24 Medicaid, therefore we will be using a 0% expected misstatement, 5% tolerable misstatement and a high level of assurance.

Using the sampling spreadsheet for large populations, we determined our sample size is 56. We then used the random number generator to select our sample. We uploaded our sample into HCA MFT and requested that HCA submit screen prints of the change request ticket. Ed compiled our request. Our testing is documented below.

## Testing:

For each selected rate change, we reviewed change request ticket to determine whether HCA Quality Assurance staff reviewed and approved the rate changes before released to production. See Edit configuration and rate change testing\_confidential Tab 'Rate Change Testing ' Large Pop'. All tickets were reviewed and approved by either Heidi Devries, IT Quality Assurance, or her backup Vicki Sutton, IT Quality Assurance. Notification to the requestor that changes were uploaded occurred after QA approval in all instances. **No exception.**

## Conclusion:

Based on our understanding, related general IT controls were in place and adequately designed to ensure that the control operated consistently during six months of the audit period. We identified the following control deficiencies:

**We identified the following weaknesses related to the Acentra Health, LLC Provider One System and Organization Controls (SOC) 2 Type 2 audit:**

- The ProviderOne vendor's SOC 2 Type 2 audit did not cover the entire fiscal year 2024. The audit did not include the first six months of the fiscal year, July 1, 2023 - December 31, 2023.
- The Authority receives and reviews the Acentra Health ProviderOne SOC 2 Type 2 audit report to determine whether there are exceptions that require corrective action. However, there are no documented procedures for receiving and reviewing the report to ensure the review is adequately and consistently performed.
- The Authority did not maintain documentation to support there was a review of the SOC 2 Type 2 audit report.



# State of Washington

**Weakness #1** V: HCA Confidential IT Controls SOC Audit (Part of ML)

We identified the following weaknesses related to the process of forcing edits through the override process:

- [REDACTED] [12]
- The Authority did not have a monitoring process in place to ensure that all claims that were forced through the override process were authorized. (Weakness #2) E: HCA ProviderOne Override IT Controls Confidential
- There were no documented procedures for performing rate changes in ProviderOne. (Weakness #3) E: HCA Non-Confidential Provider One IT Controls

Control deficiencies will be documented at LOR Summary, where the level of reporting will be determined.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at Risk Assessment.

## D.4.PRg - Human Services

*Procedure Step:* Key Control #5 (Manual)  
*Prepared By:* AMG, 10/28/2024  
*Reviewed By:* RKM, 10/29/2024

Purpose/Conclusion:

### **Purpose:**

To confirm and test the review and approval of the rates changes in ProviderOne (key control #5 for ProviderOne) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess**

## State of Washington

**control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be***

## State of Washington

*reported as findings.*

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

### **Human Services - Valuation**

**Key Control #5:** Health Care Authority reviews and approves the input of fee schedules into ProviderOne prior to being available for payment in processing in the system.

The understanding for this system is documented above in the "Controls - ProviderOne" step.

Additionally, after gaining an understanding of this key control, IT Audit identified the same general key control, documented - [IT General Controls](#)

IT identified the following control:

**Key General IT Control #4: All simple rate changes are reviewed and approved by Quality Assurance prior to being loaded into production to ensure simple rate changes function as intended.**

Therefore we will be utilizing the control confirmation preformed by Team IT Audit.

### **1. Confirmation of Key Manual Control:**

**This works was documented, reviewed and approved by Team IT Audit, see [\[IT General Controls\]](#)**

On June 3, 2024, we met with Ed Hicks, IT System Administrator, Lorena Delgado, IT System Administrator, Angela Skinner, IT System Administrator, Heidi DeVries, IT Quality Assurance, and Kari Summerour, External Audit and Compliance Manager to walkthrough and confirm Key General IT Control #4 [\[Gen IT KC confirmation system documentation client confidential\]](#).

Lorena shared her screen and began walking us through a recent rate change request (Ticket #P10062208) that was requested on May 29, 2024 by the Rate group (Kathryn Mesaros, Social Service Billing and Training Program Manager). This rate change request was to Update the rate for SA298 and edit logic for logic 30149. Because tickets sometime come with multiple requests within, this ticket also had an edit configuration update. Here, we will only focus on the rate change for SA298 which is a Procedure Rate. This specific procedure rate was being updated from \$0.01 to \$4,000 to \$0.01 to \$10,000 effective May 1, 2024.

Lorena reviewed the Excel file submitted with the ticket by the Rates group see Screen print #6 and the attached excel file containing the rate

## State of Washington

update at Screen print #7. All elements on the rate change request were accurate. Lorena then logged into ProviderOne and uploaded the rate sheet into UAT and ran ProviderOne's processing verification on the rate sheet. ProviderOne returned no errors. Lorena then logged in as an approver and approved testing. *Note: The rate does not go live until after the QA Review in the Production environment.* Once testing was complete and approved, Lorena logged in as a tester in the production environment and conducted the same process and uploaded the rate sheet into ProviderOne's processing verification, see Screen print #8. Lorena again ran the Processing verification on the rate sheet in production and when ProviderOne returned no errors, see Screen print #9, Lorena then approved the rate sheet testing in Production. Batch instance number 500105893 is for file review tracking purposes. Lorena showed us that she did not have the profile (Operations and Support System Approver) to approve rates in production. Once Lorena approved the rate sheet's testing in Production, she took a copy of the rate sheet loaded into production and uploaded it into the helpdesk and assigned the ticket to Heidi Devries, IT Quality Assurance. Heidi shared her screen and logged in with the profile Operations and Support System Approver and walked us through her review and approval. Heidi verifies that original ticket matches the approved ticket in Production and that no changes were made. Heidi also expanded the rate past two decimals and verified that the rate ends in all zeros. Heidi did not identify any necessary revisions and so she approved the rate and it was then active in ProviderOne including a definite start date of May 1, 2024 and a indefinite end date, see Screen print #10.

### Noted Weaknesses are as follows:

- We did not identify any weaknesses in the design or operation of controls.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.4.PRG - Human Services**

*Procedure Step:* Key Control #6 (Manual)  
*Prepared By:* AMG, 6/17/2024  
*Reviewed By:* BM2, 11/20/2024

## State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm and test batch reconciliations between ProviderOne and AFRS (key control #6 for ProviderOne) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

## State of Washington

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all*

# State of Washington

*control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

## **Human Services - Completeness**

**Key Control #6** - Fiscal analysts at both HCA and DSHS perform a daily reconciliation of amounts for batch interface uploads between the ProviderOne system and AFRS for AH (Payments and adjustments) and AI (Warrant cancelations or reissuances) batches.

The understanding for this system is documented above in the "Controls - ProviderOne" step.

### **1. Confirmation of Key Manual Control:**

To confirm whether daily reconciliations between ProviderOne to AFRS are performed (which would ensure complete roll-up of expenditures from the source system to AFRS), we performed the following procedures:

On May 8, 2024 we met with the following individuals from the Health Care Authority:

- Will Sogge, External Audit Liaison
- Tanya Daymon, Fiscal Analyst 3
- Cheri Gullekson, Medicaid Accounting Manager

Tanya shared her screen and walked us through the process of reconciling the P1 data to AFRS. Tanya will take a screen shot of the ProviderOne batch reconciliation report and paste it into the Excel workbook with a new worksheet for each day of the month. She will then access the AFRS - Batch Interface (BI) system and runs an AFRS batch interface report. The AFRS batch report also specifies agency, batch type, batch number,



## State of Washington

batch count, and batch amount. She will take a screen shot of this AFRS report and paste it to the same worksheet as the ProviderOne batch reconciliation report. The Fiscal Analyst verifies on the AFRS batch report that the batch date, batch number, batch count, and batch amount shown in the AFRS report matches to the ProviderOne batch report. If the batch item on both reports match, she will electronically sign the top of the worksheet where it says "Reviewer" for this batch date.

On June 11, 2024 we met with the following people from the Department of Social and Health Services:

- Rick Meyer, External Audit and Compliance Manager
- Laura Benson, Fiscal Analyst 5, Cash Unit Supervisor
- Christina Choate, Program Services Manager
- Christie Johnson, Administrative Services Manager
- Ashleigh Thompson, Fiscal Analyst 3

Laura shared her screen and walked us through the process of reconciling the P1 data to AFRS. She stated normally Jesrie Beane, Fiscal Analyst, would reconcile the workbooks and if she is not available, Ashleigh Thompson would reconcile the data if Jesrie is gone for more than a day. Laura explained that Jesrie will take a screen shot of the ProviderOne batch reconciliation report and paste it into the Excel workbook with a new worksheet for each day of the month. She will then access the AFRS - Batch Interface (BI) system and run an AFRS batch interface report. The AFRS batch report also specifies agency, batch type, batch number, batch count, and batch amount. She will take a screen shot of this AFRS report and paste it to the same worksheet as the ProviderOne batch reconciliation report. The Fiscal Analyst verifies on the AFRS batch report that the batch date, batch number, batch count, and batch amount shown in the AFRS report matches to the ProviderOne batch report. If the batch item on both reports match, she will electronically sign the top of the worksheet where it says "Reviewer" for this batch date.

### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.4.PRG - Human Services**

# State of Washington

*Procedure Step:* Risk Assessment

*Prepared By:* AMG, 11/6/2024

*Reviewed By:* RKM, 12/2/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

1. Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to a material misstatement, assuming that there are no related controls. Inherent risk can be thought of as the "threat" of misstatement. Inherent risk exists independently of control risk (the level of threat exists independent of the level of vulnerability to threats). Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*
  - *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

## State of Washington

- *Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*
- *Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*
- *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*
  - *Are there substantial pressures or motivations to misstate the balance?*
- *Inherent Risk due to Misappropriation*
  - *Is the account balance or transaction class susceptible to sizable misappropriation?*
- *Inherent Risk due to Non-Compliance*
  - *Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*
  - *Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*
  - *Are there any motivations or pressures to not comply?*

2. Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and testing (if applicable). If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*In order to set control risk to LOW, general controls would also need to be tested to provide evidence of the consistent operation of automated controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body.*

***All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

## State of Washington

- 3. Assess the risk of material misstatement for each relevant assertion for each material line item. The risk of material misstatement is a combination of the auditor's separate assessment of inherent and control risk.

*The Risk of Material Misstatement is a combined assessment of inherent and control risk based on auditor's judgment. If inherent and control risk are assessed differently, it is a matter of professional judgment as to whether the combined assessment is moderate or if one factor outweighs the other.*

4. Design a substantive testing strategy that addresses the relevant assertion in all significant transaction streams included within the material line item.

*In addition to identifying what to audit (material balances) and what to audit for (relevant assertions), planning has also identified how much to audit (risk of material misstatement). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done.:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- Rights and Obligations - High
- Valuation - High
- Completeness - High

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

## State of Washington

- ProviderOne

**Rights and Obligations/Valuation/Completeness - MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level

**MAX** - While we have performed tests for the assertions above, general internal controls for the ProviderOne system can partially be relied due to the ISOC 2, Type II report for the fiscal year. As such, we identified the following weaknesses regarding the general controls during the fiscal year for the SOC report:

- The ProviderOne vendor's SOC 2 Type 2 audit did not cover the entire fiscal year 2024. The audit did not include the first six months of the fiscal year, July 1, 2023 - December 31, 2023.
- The Authority receives and reviews the Acentra Health ProviderOne SOC 2 Type 2 audit report to determine whether there are exceptions that require corrective action. However, there are no documented procedures for receiving and reviewing the report to ensure the review is adequately and consistently performed.
- The Authority did not maintain documentation to support there was a review of the SOC 2 Type 2 audit report.

Due to the identified weaknesses, we will be issuing a recommendation, see V: HCA Confidential IT Controls SOC Audit (Part of ML) See, IT General Controls for full analysis of gernal IT Controls.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

- Rights and Obligations - High
- Valuation - High
- Completeness - High

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

#### **A. Substantive test to meet the Rights and Obligations and Valuation assertions:**

Select a random sample of ProviderOne transactions and perform the following tests:

- Test 1: Determine whether the recipients are eligible (Rights & Obligations) at the time of service based upon their insurance group
- Test 2: Determine whether the providers are eligible to provide services and bill Medicaid at the time of service (Rights & Obligations)
- Test 3: Determine whether the services are allowable per State Plan (Rights & Obligations)

## State of Washington

- Test 4: Determine whether the paid amounts are correctly determined or calculated based on authorized rate or fee schedule (Valuation)

Additionally, we will select a sample of P1 IT helpdesk tickets and review the process of the rate change review, approval, and upload to the system and perform testing to determine if the Authority followed their procedures to ensure rates were being reviewed and applied correctly.

### **B. Substantive test to meet the Completeness assertion:**

Select a random sample of P1 and AFRS batch reconciliation reports (daily reconciliation reports) and performed testing on the sample reports to determine whether total amounts in the ProviderOne batch report tie to AFRS Batch Interface Report.

### **C. Completed in-house CAATs (computer assisted audit techniques) work**

This allowed us to look at the actual payments made during the audit period, and determined that ProviderOne processed payments as based on our understanding of automated controls in ProviderOne system. This was a re-performance of the controls on a large scale, which provided us with much more assurance if the controls were working as described. Additionally, since we reviewed actual payments, we also considered this as dual purpose testing because it provided us with a great deal of substantive evidence as well.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **D.4.PRG - Human Services**

*Procedure Step:* Substantive Test  
*Prepared By:* AMG, 11/15/2024  
*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:
---------------------

#### **Purpose:**

To determine whether all expenses/expenditures incurred during the period were reported. (Completeness)

To determine whether the agency would have legal authority to make reported expenses/expenditures. (Rights & Obligations)

To determine whether expenses/expenditures were reported at properly valued or calculated amounts. (Valuation)

# State of Washington

## **Sources:**

DSHS documentation provided by Rick Meyer, External Audit Compliance Manager

HCA documentation provided by Willl Sogge, External Audit Liaison

ProviderOne - HCA System that store Medicaid Information and Documentation

## **Conclusion:**

- **Test 1:** Claims processed within ProviderOne were made to eligible clients (based upon their insurance group, recipient aid category, and enrolled managed care program, as applicable) on the date of service.
  - No exceptions noted.
- **Test 2:** Claims processed within ProviderOne were made by eligible providers (based upon their status and taxonomy group) on the date of service.
  - No exceptions noted.
- **Test 3:** Claims processed within ProviderOne were allowable per the State Medicaid Plan.
  - No exceptions noted.
- **Test 4:** Claims were paid at the correct amounts are correctly determined and calculated based on authorized rate or fee schedule.
  - No exceptions noted.

Testing Strategy:

## **Completeness**

The following is a list of **considerations** for testing the completeness assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Detail Roll-Up**

- Compare totals from general ledger to accounts payable, payroll or other subsidiary software modules.
- Review the government's reconciliation of general ledger to subsidiary systems.

### **Cut off / Improper Expense Recognition**

- Scan expenditures recorded 1-3 months before and/or after fiscal year end (expenditures not charged to the current period). Based on the scan, test selected or sampled expenditures to determine if the expense should have been reported in the current period.
- Inquire with AP clerks regarding invoices held, but not entered as of year-end (ie: due to pending litigation or disputes).

### **Unrecorded Expenses**

- If the entity reconciles recorded revenues and expenses to bank activity, then reviewing monthly reconciliations and evaluating or testing reconciling items.

### **Accounts Payable**

## State of Washington

- If entity uses a warrant clearing account for vendor payments, review the entity's year-end reconciliation of recorded vendor payments with disbursements from the clearing account.
- Review edit check reports from the AP system that might indicate missing payments.

### **Payroll**

- If entity uses a payroll clearing account, review the entity's year-end reconciliation of recorded payroll with disbursements from the payroll clearing account.
- Perform an expected payroll test by taking the prior audited payroll amount and adjusting it for expected changes.

*The analysis should consider changes in employees, COLA increases, salary scale increases if automatic, changes wages or benefits due to changes in policy or union negotiations changes, etc. Sources for these expectations should be obtained apart from the payroll records that are being tested. Since the auditor would not expect to be able to precisely predict payroll, the auditor should document a reasonable range within which actual payroll is expected to vary from the auditor's prediction.*

- If the board directly approves salaries for a significant amount of employees, verify whether the actual salaries for these employees is within an expected reasonable range of the approved salary.
- For small entities, compare payroll by employee to known employees per observation, organization charts or a phone list.
- Review edit check reports from the payroll system that might indicate missing payments.

### **Unrecorded Liabilities**

- Evaluate liabilities directly related to expenses for completeness. See the completeness steps for current and non-current liabilities for testing considerations.

*For example, if the entity reports a self-insurance liability, the auditor might evaluate whether the change in the liability (and related expense) was determined and recorded. If no liability was reported, then the auditor might determine whether such a liability (and associated expense) should have been reported.*

**OPEB** - auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

### **Removing Expenses from Accounting Records**

- Search for manual journal entries that credit (decrease) expenditures. Consider testing selected transactions.



## State of Washington

- Identify transactions that void, cancel, or manually adjust transactions in subsidiary AP or payroll systems. Auditors may conclude that the total amount of such transactions are trivial or otherwise reasonably small. Or auditors may sample or select transactions for testing.

*Also see considerations under the "Not recording expenses" section.*

### **Interfund Expenses**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

### **Rights and Obligations**

The following is a list of **considerations** for testing the rights and obligations assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

- Review selected expenses/expenditures to determine whether the entity had legal authority to make the payments or incur the liability.
- If disbursements for different entities are made out of the same bank account, review the entity's reconciliation of accounting records to disbursements to verify that only expenditures of the entity were reported by that entity.
- Compare vouchers audited and certified by the auditing officer to the warrant register or review documentation for selected or sampled vouchers to determine whether expenses/expenditures were audited and certified in accordance with RCW 42.24.080.
- Compare board-approved vouchers to the warrant register or review documentation for selected or sampled vouchers to determine whether expenses/expenditures were properly approved by the governing body.
- Test selected or sampled transactions for compliance (allowability, eligibility, etc) with applicable restrictions or requirements.

*NOTE: this test may be combined with expenditure tests for other attributes. For example, expenditure testing for accountability or single audit purposes would normally also be considered testing for the rights & obligations assertion.*

### **Expenditures related to Joint Ventures or Other Arrangements**

- Review forming documents and agreements to verify expenditures for obligations of the venture.

**OPEB** - Auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - Auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

## State of Washington

### **Valuation**

The following is a list of **considerations** for testing the valuation assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests:

- Verify that payroll calculations are correct.
- If not already covered as part of control testing, verify that payroll software used correct rates.
- If not already covered as part of control testing, verify that accounts payable software used correct rates for calculating sales tax.
- Review calculation of any estimated expenses.
- Review related-party transactions to determine whether expense/expenditure transactions were correctly calculated.

### **Landfill Closure & Post-Closure Expenses**

*See the valuation testing strategy for non-current liabilities..*

**OPEB** - Auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - Auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

Guidance/Criteria.*
---------------------

### **Medicaid Specific:**

**Medicaid State Plan:** <https://www.hca.wa.gov/about-hca/programs-and-initiatives/apple-health-medicare/medicaid-title-xix-state-plan>

**Provider billing guides and fee schedules:** <https://www.hca.wa.gov/billers-providers-partners/prior-authorization-claims-and-billing/provider-billing-guides-and-fee-schedules>

**DSHS Rates (DDA/HCS/Nursing):** <https://www.dshs.wa.gov/altsa/management-services-division/office-rates-management>

### **Completeness**

#### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.6.13](#) Utility Tax (*applies only to cities*)** - should be accounted for as a revenue in the general fund (3164000) and expenditure in the utility fund (53P0040), if the utility passes the tax on to its customers then the additional charges should be recognized as revenue (343P000) directly in the utility fund not in the general fund

**BARS [3.8.6](#) Use of Payroll and Claims Funds**

# State of Washington

## **Rights and Obligations**

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.8.5](#) Voucher Certification and Approval** - prescribes the form and manner of the audit and certification

**BARS [3.8.6](#) Use of Payroll and Claims Funds**

**RCW [42.24.080](#)** - describes statutory audit, certification and approval requirements

**RCW [42.24.180](#)** - gives the only exception to payment of claims prior to approval by the legislative body. In absence of meeting these requirements, no expenditure can be made without prior approval of the legislative body

## **Valuation**

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.8.6](#) Use of Payroll and Claims Funds**

Record of Work Done:

### **Substantive tests performed to meet the Valuation Assertion:**

To test whether HCA adequately reviews and approves the input of fee schedules and changes into ProviderOne prior to them being available for payment processing in the system.

**Population:** We generated populations of rate upload files for both fee-for-service and managed care within ProviderOne by pulling the following exports:

#### **Fee For Service:**

Rate Settings -> Rate Group drop down:

- Provider Rates- 9,102 rate changes
- Program Rates- No rate changes

# State of Washington

- Group Rates- 1 rate change
- Proc/Svc/Revenue Rates- 36,841 rate changes
- Client Rates- 12,326 rate changes
- Taxonomy Rates- 2,080 rate changes
- DRG Value Rates- No rate changes

Filter By: Upload Date **07/01/2023 to 06/30/2024** And: File Name % And Status: **Approved**.

## **Managed Care:**

Managed Care -> PMPM Rate Configuration and Select View Summary Rate Report. Then use the Filter by drop down and select Generate Date and input **07/01/2023 to 06/30/2024**. There were 480 rate changes

The process of rate change review, approval, and upload are similar between the MC and FFS rates, but the requests originate from different teams. We combined all FFS and MC rate change files into a single population to draw our sample. There were 60,365 total rate changes. Because multiple rate changes are included in a ticket, we summarized our population by File Name, and Upload date. This results in 686 file names or tickets.

**Sample Selection:** There were 686 tickets for rate changes in total during state fiscal year 2024. Based upon the sample criteria (population quantity/amount, expected misstatement, tolerable misstatement, and level assurance) we determined a sample size of 56 for each testing population. We will be using the same testing criteria for the FY24 Medicaid, therefore we will be using a 0% expected misstatement, 5% tolerable misstatement and a high level of assurance.

Using the sampling spreadsheet for large populations, we determined our sample size is 56. We then used the random number generator to select our sample. We uploaded our sample into HCA MFT and requested that HCA submit screen prints of the change request ticket. Ed compiled our request. Our testing is documented here, see [Edit configuration and rate change testing\\_confidential](#).

## **Testing Results:**

For each selected rate change, we reviewed change request ticket to determine whether HCA Quality Assurance staff reviewed and approved the rate changes before released to production. See Tab 'Rate Change Testing ' Large Pop'. All tickets were reviewed and approved by either Heidi Devries, IT Quality Assurance, or her backup Vicki Sutton, IT Quality Assurance. Notification to the requestor that changes were uploaded occurred after QA approval in all instances. **No exception noted.**

## **Substantive tests performed to meet the Completeness Assertion:**

We selected a random sample of P1 and AFRS batch reconciliation reports (daily reconciliation reports) and performed testing on the sample reports to determine whether total amounts in the ProviderOne batch report tie to AFRS Batch Interface Report, see [FY24 Human Services FS](#)

# State of Washington

## Sampling Spreadsheet

For the randomly selected days we obtained ProviderOne batch reconciliation reports (report 1280) and AFRS Batch Interface Reports (screen C105P070) and confirmed that the quantity of records and total batch amounts in the ProviderOne batch report tied to the AFRS Batch Interface report, ensuring the completeness of interfacing for the claim payments.

To test whether daily reconciliations between ProviderOne to AFRS are performed (which would ensure complete roll-up of expenditures from the source system to AFRS), we performed the following procedures:

### ***Population***

As the reconciliations are performed daily, we identified workdays (non-weekends and non-holidays) between 7/1/2023 and 6/30/2024, resulting in a total of 249 workdays, see FY24 Human Services FS Sampling Spreadsheet. We consider our testing to be sufficient as the process is the same for the entire year and our population is sufficiently large to opine on.

### ***Selection***

As the reconciliations are the same between the two agencies, we determined each agency will be tested separately in order to determine if they each perform the daily reconciliations during the year. Based upon the small sampling spreadsheet with tolerable misstatement of 5% and 0% expected failure rate, the stated sample size is 24; this is the same sample size as the Control Statistical Sample with the same parameters. We randomly selected 24 reconciliation workdays for both DSHS and HCA.

### Testing Results:

- The agencies performed a reconciliation of the prior day between ProviderOne report 1280, for batch types AH/AI - **Both agencies performed reconciliations between AFRS and ProviderOne within the ProviderOne settlement date, no issues noted.**
- The ProviderOne report 1280 amounts reconciled to the AFRS Batch Interface Logs - We reconciled the AFRS batch interface amounts to the ProviderOne 1280 reports each day with **with no differences between the batched amounts noted.**

ProviderOne transactions batched completely to AFRS based upon amounts and quantities reported on the P1 report 1280 and AFRS Batch Interface Reports (screen C105P070) for batch types AH/AI (warrant related). **No issues noted.**

### **Random Sample Selection Procedures for Claims/Premiums for Valuation and Rights & Obligations:**

#### ***Populations***

HCA provided ProviderOne claim data covering the 7/1/2023 through 6/30/2024 time period. The claim data information, including total quantity of transactions and paid amounts, is summarized at [FY24 Human Services Stratification]. To address the risk of material misstatement (MAX for Rights/Obligations and MAX for Valuation), we set the assurance needed to **high** and set a **0% expected misstatement rate**. Because this test is also used for the Statewide Single Audit, the **tolerable misstatement was set for 5%**. This resulted in 59 sample items for testing.

# State of Washington

Due to the nature of claim transactions, we determined testing required sub-sampling for various populations. For the agencies, we noted the following populations of claims:

- ProviderOne Claims - DSHS - Social Services
- ProviderOne Claims - DSHS - Medical Service Claims (Fee for Service)
- ProviderOne Claims - HCA - Medical Service Claims (Fee for Service)
- ProviderOne Claims - DSHS - Managed Care Claims
- Provider One Claims - HCA - Managed Care Claims

We determined that the claims for DSHS Managed Care (0.49%) were insignificant to the balance of the ProviderOne claims and excluded this subset from testing. We additionally excluded negative values to \$1 claims from the sample frames and claims under \$10 (DSHS Fee for Service sample frame) due to their insignificance. For each sampling frame, we stratified the transactions into quartiles (to a reasonable degree) and/or along the natural histogram of the populations and allocated the 59 transactions pro-rata based upon each stratum's total amount to the overall sampling frame.

Samples were pulled by IT Audit using a stratified sampling method documented in:

**Fee for Service:** [Sampling for ProviderOne Claims](#)

**Managed Care:** [Sampling for ProviderOne Managed Care](#)

**Testing** (Sample results are summarized below; detailed testing notes and procedures are on subsequent tabs that are referenced)

**DSHS Social Services:** [CONFIDENTIAL FY24 Human Services Detailed Testing](#)

**DSHS Fee for Service:** [CONFIDENTIAL FY24 Human Services Detailed Testing](#)

**HCA Fee for Service:** [CONFIDENTIAL FY24 Human Services Detailed Testing](#)

**HCA Managed Care:** [CONFIDENTIAL FY24 Human Services Detailed Testing](#)

## **Substantive tests performed to meet the Rights & Obligations assertion:**

### *ProviderOne Claim Testing Procedures*

- **Test 1:** Determine whether the recipients are eligible at the time of service based upon their insurance group (client eligibility)
  - Medicaid Eligibility: ProviderOne client information to ensure that service beneficiaries were enrolled as an eligible Medicaid recipient (Insurance Type = MC: Medicaid) on the date(s) of service.
  - Recipient Aid Category Eligibility: We accessed ProviderOne client information to ensure that service beneficiaries were enrolled within the corresponding RAC on the date(s) of service for which the service was coded.
  - Managed Care (in addition to above for Medicaid for HCA - Managed Care sample): We accessed ProviderOne client information to ensure that service beneficiaries were enrolled in one of the Washington Managed Care organizations (Insurance Type = HM: Health Maintenance Organization) on the date of service/premium payment.

## State of Washington

- **Test 2:** Determine whether the providers are eligible to provide services and bill Medicaid at the time of service (provider eligibility)
  - Eligible Provider: We accessed ProviderOne provider information to ensure that providers (overall organization) were enrolled as an active (eligible) provider on the date of service.
  - Taxonomy (N/A for Managed Care): We accessed ProviderOne provider information for the claim provider to ensure that the provider was approved for the provider-type and speciality (taxonomy code) on the date of service.
  - Service Eligibility (N/A for Managed Care): We reviewed the claimed proc/svc code history and modification codes to ensure that the proc/svc was approved as part of the listed taxonomy on the date of service.
- **Test 3:** Determine whether the services are allowable per State Plan (service eligibility)
  - We reviewed the descriptions of services for the transactions using various attributes such as procedure code and reviewed the Washington State Medical State Plan, Attachment 3 and State Billing guides to determine whether the services were under a covered service category, e.g. Inpatient hospital, dental services, etc.
  - For HCA - Managed Care, the majority of samples were premium payments which are for a method of Medicaid administration. This includes the premium withholding release payments for prior premiums when the MCO met the requirements of the Value Based Purchasing targets.

*IT Dual Purpose Testing* [Key Controls #1 - 4 Edit Checks (Automated) - FY24 Dual Purpose Procedure Code Testing - Edit population, selection and testing client confidential]

- **IT Test 1:** Was the recipient eligible to receive the medical assistance services on the specific service dates?
  - CAATS/IT Procedures: IT audit performed editing testing and checks for a selection of error codes related to the validity of a claim's client.
- **IT Test 2:** Was the provider enrolled as an active (eligible) provider on the specific service dates?
- CAATS/IT Procedures: IT audit performed edit testing and checks for a selection of error codes related to the validity of a claim's provider.
- **IT Test 4:** Was the assistance service listed as an allowable service in the Medicaid State Plan?
  - CAATS/IT Procedures: IT audit performed edit testing and checks for a selection of error codes related to the validity of a claim's procedure code.

### **Substantive tests performed to meet the Valuation assertion:**

*ProviderOne Claim Testing Procedures*

- **Test 4:** Determine whether the paid amounts are correctly determined or calculated based on authorized rate or fee schedule (service paid rate)
  - HCA Fee-for-service - We reviewed billing guides and fee schedules, point of sale support, and rates within ProviderOne to recalculate the fees. Generally:

## State of Washington

- Pharmacy claims: We reviewed point-of-sale support to ensure that the POS system and ProviderOne paid the lesser of drug costs based upon various reference tables for the amount paid.
- Medicare Crossover claims: We ensured that ProviderOne elected the lesser of the allowable Medicaid (as computed) and Medicare amounts and deducted Medicare payments for the amount paid.
- Inpatient/Outpatient claims: We reviewed billing and fee schedules to ensure that ProviderOne used the correct factors (NPI conversion factors, EAPG weights, DRG weights, etc.) based upon claim information and recalculated the paid amount.
- Other Claims: We reviewed specific billing guides and fee schedules to ensure that ProviderOne used the correct rates and calculations for the amount paid.
- DSHS Fee-for-service and Social Services - We reviewed billing guides and fee schedules, Provider rates and authorized rates (from prior authorizations) within ProviderOne and recalculated the paid amount.
- HCA Managed Care -
  - Service Based Enhancement Claims - We ensured that the Provider's rate for the applicable charge mode was used for the payment amount and recalculated the paid amount.
  - Premiums - We reviewed client cohort information to ensure that the appropriate rates/factors were used and recalculated the client's monthly premium. This included withhold release TCNs (void old monthly premium TCN with amount withheld and processing a related TCN for a percentage release of the withhold amount).

### *IT Dual Purpose Testing* [Key Controls #1 - 4 Edit Checks (Automated) - FY24 Dual Purpose Procedure Code Testing]

- **IT Test 3:** Determine whether the paid amounts are correctly determined or calculated based on authorized rate or fee schedule (Valuation)
  - CAATS/IT Procedures: IT audit performed edit testing and checks for a selection of error codes related to the valuation of a claim.

### Testing Results:

#### *ProviderOne Claim Testing Results*

- **Test 1:** Claims processed within ProviderOne were made to eligible clients (based upon their insurance group, recipient aid category, and enrolled managed care program, as applicable) on the date of service.
  - No exceptions noted.
- **Test 2:** Claims processed within ProviderOne were made by eligible providers (based upon their status and taxonomy group) on the date of service.
  - No exceptions noted.
- **Test 3:** Claims processed within ProviderOne were allowable per the State Medicaid Plan.
  - No exceptions noted.
- **Test 4:** Claims were paid at the correct amounts are correctly determined and calculated based on authorized rate or fee schedule.



## State of Washington

- No exceptions noted.

### D.4.PRG - Human Services

*Procedure Step:* Sampling for ProviderOne Claims

*Prepared By:* JMT, 9/18/2024

*Reviewed By:* SHW, 11/5/2024

Purpose/Conclusion.:

**Purpose:**

To document sample design and methodology.

**Source:**

ProviderOne Claims data

**Conclusion:**

We have documented the sample design and methodology.

Testing Strategy.:

Guidance/Criteria.:

Record of Work Done.:

**AUDIT OBJECTIVE**

The audit objective was to determine if Claims payments processed through ProviderOne are legitimate.

**SAMPLE DESIGN AND METHODOLOGY**

The samples of ProviderOne Claims transactions were produced by the IT Audit Data Analysis team using data provided by the Health Care

# State of Washington

Authority (HCA).

HCA provided the full year (7/1/2023 - 6/30/2024) claims data on July 10, 2024 (social service claims) and August 16, 2024 (medical claims).

A document summarizing the total dollars and records received for FY24 was created and can be seen at [[FY24\\_ACFR\\_StratifiedSummaries](#)] (see tabs "DSHS SS Claims Summary" for the social service claims summary; "DSHS Med Claims Summary" and "HCA Med Claims Summary" for the medical claims summaries). Team Financial Audit (FA) Human Service line item auditors determined the amounts in these spreadsheets were reasonable based upon their general expectations of Medicaid expenditures during a fiscal year.

Team IT Audit also performs data reliability steps on all ProviderOne data received from HCA. Since the ProviderOne data mainly supports the Statewide Single Audit for the Medicaid program, all of the data reliability work is documented in that project (S1Medicaid-SA24 in V.4). In general, the following items are considered when determining the reliability of data:

- Record count of the dataset agrees to the record count provided by HCA.
- Fields requested are included in the dataset.
- Dataset covers the expected timeframe.
- Field values agree with data dictionary.
- The frequency count of values in a field are in a reasonable range.
- The minimum and maximum values of fields are in a reasonable range.
- Blank (or NULL) values do not appear in fields that should not contain missing information.
- Dataset does not contain duplication.
- Comparison of records in the dataset to the source ProviderOne system.

Based upon the various data reliability steps performed, it was determined the data used for testing was complete and accurate.

## **CHARACTERISTICS TO BE MEASURED**

We based our determination as to:

- Whether the recipients are eligible.
- Whether the providers are eligible to provide services.
- Whether the services are allowable per State Plan.
- Whether the paid amounts are correctly determined or calculated based on authorized rate or fee schedule in ProviderOne.

## **IT Audit Deliverables:**

## State of Washington

The first item provided to Team FA includes stratified summary tables for the claims and Managed Care premium payments split out by agency (DSHS and HCA). From these summaries, Team FA determines the final stratifications and sample sizes. Based on this information, IT Audit then pulls samples from the data populations and provides those to Team FA. For FY24, all samples will be pulled from the full year data and the social service and medical claims populations will be sampled from separately.

### Full Year Social Service Summary

IT Audit created summary tables by agency for the social service claims population between July 1, 2023 and June 30, 2024 [see [FY24 ACFR StratifiedSummaries](#)]. (see tab "DSHS SS Claims Summary").

The queries written to create the summary tables can be seen at [\[SS Claims Summary Queries\]](#).

### Full Year Medical Summary

IT Audit created summary tables by agency for the medical claims population between July 1, 2023 and June 30, 2024 [see [FY24 ACFR StratifiedSummaries](#)]. (see tabs "DSHS Med Claims Summary" and "HCA Med Claims Summary").

The queries written to create the summary tables can be seen at [\[Med Claims Summary Queries\]](#).

### Full Year Social Service Sample

Sample selections were made based upon the stratification and sample sizes provided by Team FA [see [FY24 Human Services Stratification](#)]. The population included all social service claims paid by Medicaid during FY24 (minimum \$1). The selected records were provided to Team FA via the internal network in a spreadsheet titled "!2024\_ACFR\_Samples\_SS\_Claims" due to the inclusion of confidential information. The queries written to select the samples can be seen at [\[SS Claims Sample Selection Queries\]](#).

### Full Year Medical Sample

Sample selections were made based upon the stratification and sample sizes provided by Team FA [see [FY24 Human Services Stratification](#)]. The population included all medical claims paid by Medicaid during FY24 (minimum \$1). The selected records were provided to Team FA via the internal network in a spreadsheet titled "!2024\_ACFR\_Samples\_Med\_Claims" due to the inclusion of confidential information. The queries written to select the samples can be seen at [\[Med Claims Sample Selection Queries\]](#).

## D.4.PRG - Human Services

*Procedure Step:* Sampling for ProviderOne Managed Care

*Prepared By:* JMT, 9/18/2024

*Reviewed By:* SHW, 11/5/2024

# State of Washington

Purpose/Conclusion.:

**Purpose:**

To document sample design and methodology.

**Source:**

ProviderOne Managed Care data

**Conclusion:**

We have documented the sample design and methodology.

Testing Strategy.:

Guidance/Criteria.:

Record of Work Done.:

**AUDIT OBJECTIVE**

The audit objective was to determine if Managed Care payments processed through ProviderOne are legitimate.

**SAMPLE DESIGN AND METHODOLOGY**

The samples of ProviderOne managed care transactions were produced by Team IT Audit using data provided by the Health Care Authority (HCA).

HCA's vendor, CNSI, provided the full year (7/1/2023 - 6/30/2024) managed care data on August 16, 2024.

A document summarizing the total dollars and records received for FY24 was created and can be seen at [FY24 ACFR StratifiedSummaries] (see tabs "DSHS MC Summary" and "HCA MC Summary" for the managed care summaries). Team FA Human Service line item auditors determined the amounts in these spreadsheets were reasonable based upon their general expectations of Medicaid expenditures during a fiscal year.

Team IT Audit also performs data reliability steps on all ProviderOne data received from HCA. Since the ProviderOne data mainly supports the Statewide Single Audit for the Medicaid program, all of the data reliability work is documented in that project (S1Medicaid-SA23 in V.4). In

# State of Washington

general, the following items are considered when determining the reliability of data:

- Record count of the dataset agrees to the record count provided by HCA.
- Fields requested are included in the dataset.
- Dataset covers the expected timeframe.
- Field values agree with data dictionary.
- The frequency count of values in a field are in a reasonable range.
- The minimum and maximum values of fields are in a reasonable range.
- Blank (or NULL) values do not appear in fields that should not contain missing information.
- Dataset does not contain duplication.
- Comparison of records in the dataset to the source ProviderOne system.

Based upon the various data reliability steps performed, it was determined the data used for testing was complete and accurate.

We will rely on the totals from the first six months for determining sample size as we expect the amounts to stay consistent throughout the fiscal year.

## **CHARACTERISTICS TO BE MEASURED**

We based our determination as to:

- Whether the recipients are eligible.
- Whether the providers are eligible to provide services.
- Whether the services are allowable per State Plan.
- Whether the paid amounts are correctly determined or calculated based on authorized rate or fee schedule in ProviderOne.

## **IT Audit Deliverables:**

The first item provided to Team FA includes stratified summary tables for the claims and Managed Care premium payments split out by agency (DSHS and HCA). From these summaries, Team FA determines the final stratifications and sample sizes. Based on this information, IT Audit then pulls samples from the data populations and provides those to Team FA. For FY24, all samples will be pulled from the full year data.

### Full Year Summary

IT Audit created summary tables by agency for the managed care population between July 1, 2023 and June 30, 2024 [see FY24\_ACFR\_StratifiedSummaries]. (see tabs "DSHS MC Summary" and "HCA MC Summary" for the managed care summaries). The queries written to create the summary tables can be seen at [MC Claims Summary Queries].

# State of Washington

## Full Year Sample

Sample selections were made based upon the stratification and sample sizes provided by Team Financial Audit [see [FY24 Human Services Stratification](#)]. The population included all Managed Care premium Medicaid transactions during FY24 (minimum \$1). We did not include any transactions that net to zero, nor did we include any transactions identified as a replaced transaction. The selected records were provided to the Team via the internal network in a spreadsheet titled "!2024\_ACFR\_Samples\_MC" due to the inclusion of confidential information. The queries written to select the samples can be seen at [\[MC Claims Sample Selection Queries\]](#).

## D.5.PRG - Federal Grants in Aid

*Procedure Step:* Summary & Conclusion

*Prepared By:* SRC, 10/22/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

## State of Washington

*If the results of substantive testing indicate a need to change control risk, auditors should also update the [Permanent File](#) by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

## State of Washington

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **D.5.PRG - Federal Grants in Aid**

*Procedure Step:* Understanding of Line Item

*Prepared By:* SRC, 8/16/2024

*Reviewed By:* RKM, 8/22/2024



# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associated with the line item.
- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new

## State of Washington

one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

There were no prior audit exceptions for the Federal Grants-in-Aid line item in the prior ACFR.

#### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

**Note:** We rely on work performed at the fund level to substantiate at the government-wide level.

#### **Significant Changes**

We inquired with:

- **HCA:** Laura Roberts, Federal Claims Supervisor and Jill Arlow, Deputy Section Manager (Federal Financial Reporting Section). Both confirmed that the process for the federal draw-downs and recording of the revenues have not changed.
- **DSHS:** Christina Choate, Program Services Manager, and Christie Johnson, Administrative Services Manager. Both confirmed that the process for the federal draw-downs and recording of the revenues have not changed.

# State of Washington

Federal cash revenues are recorded when agencies draw down federal cash (cash receipts) based upon the cash payments of federal program expenditures:

## *Cash Revenues - GL3210*

- **Cash Draw Downs (Cash Receipts)** - Agencies receive reimbursement funds from federal grants equal to cash expenditures less any prior year liquidations. Liquidations occur when revenues accrued in a prior year are paid out in the current year. The liquidation does not impact current year expenditure and revenue account balances as it is a cash payout for the accrual. The liquidation decreases the total cash draw balance and the revenue receivable balance.
- **Federal Cash Revenue:** Federal grantors pay out reimbursements owed to agencies once the agencies have paid for the expenditures. Cash received is based upon both cash expenditures and liquidations. Federal cash revenue, thus, equals the total of federal cash receipts less any cash received for liquidations of prior accrued expenditures.

## *Accrued Revenues - GL3205*

- Agencies accrue federal revenue up to the total allowed federal expenditure amounts as the federal grantors will reimburse agencies for those allowed expenditures that they have paid. Federal accrual revenues are recorded monthly. Accruals for June are handled separately due to the fiscal year end process.
- Monthly accruals are recorded as XX batches which are automatically reversed in the subsequent month with XY batches.
- June accruals are initially processed at the end of the fiscal year, but periodically updated with JV runs up until phase II close to calculate the most current and accurate accrual to record, using up-to-date enterprise reporting reports.

## Composition Analysis

We reviewed FY23 reports from the ACFR database for federal revenue (Roll up fund FAA, Major Source 03, GL Account 32%) as of 8/12/24 and noted that the following agencies composed 75.8% of the FGIA revenues (\$17,382,071,367):

- HCA: \$9,586,337,953, 41.8%
- DSHS: \$7,795,733,413, 34%

Amounts recorded in the Federal Grants in Aid line item are primarily the combined revenue of the Department of Social and Health Services (DSHS) and Health Care Authority (HCA), received for federal program expenditure reimbursements administered by both agencies. The total federal revenue balance contains cash revenues (GL3210), accrued revenues (GL3205) and revenue adjustments (GL3225).

We further analyzed the sources (federal administration) of above agencies' revenues and grouped the revenues by subsourse.

## **HCA**

HCA's revenue is primarily from Medicaid revenue subsources (D\*, N\*, Q\*, T\*, U\*), totaling approximately \$9.403 billion (63.7%) and Insurance

# State of Washington

Premiums, totaling \$4.843 billion (32.8%) for FY23.

## **DSHS**

DSHS's revenue is primarily from:

- Department of Agriculture - These are revenues associated with SNAP administration, totaling approximately \$131.3 million (2.8%). DSHS records the reimbursement draws to GL3225 for SNAP.
- Department of Health and Human Services - The primary revenues from DHHS are for the Medicaid program (see subsources above), totaling approximately \$4.276 billion (92.7%).

These percentage compositions are expected as DSHS is the administrator of the SNAP program and has Medicaid services within DDA and ALTSA administrations.

## **(3) Updates to Significant Account Matrix:**

No updates to the Significant Account Matrix are necessary. Revenues for the line items are in expected agencies and programs.

## **D.5.PRG - Federal Grants in Aid**

*Procedure Step:* Controls - HCA  
*Prepared By:* SRC, 8/20/2024  
*Reviewed By:* RKM, 9/27/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

## State of Washington

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

## State of Washington

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

## [Financial Statement Audits](#) Planning Guide

Record of Work Done:

Internal controls for the Federal drawn down (HCA) process address the following balance(s):

- **General Fund - Federal Grants in Aid**
- **Governmental Activities - Operating Grants and Contributions: Human Services**

Primarily reimbursement from the Federal government for Medicaid - Payments of medical treatment of eligible, low-income persons.

For the following assertions:

- **Rights and Obligations** - Federal draw-down requests may not be based on actual grant expenditures in accordance with federal cash management requirements.
- **Valuation** - Federal Grant draw-down requests may not be correctly calculated.

### **Gain an Understanding of Internal Controls**

We met with:

- Laura Roberts, Federal Claims Supervisor
- Jill Arlow, Deputy Section Manager (Federal Financial Reporting Section)
- William Sogge, External Audit Liaison

A high level summary of the draw process is as follows:

- **Federal Revenue Draws:** The cash draw amount determination is based on actual cash and liquidation expenditures as recorded in AFRS. AFRS account coding identifies amounts to calculate the federal and state share of each expenditure based on match rates (FMAP) received from the appropriate federal awarding agency.
- **Draw Frequency:** HCA requests cash draws in the period the expenditures were incurred to ensure timely and regular draws. Timing frequency for draws varies:
  - Weekly (Monday) for the Title XIX services.
  - Bi-weekly (Payday) for all other federal awards to coincide with state payroll; this will include the administrative reimbursement for the program.

## State of Washington

- Monthly (Premium) for ProviderOne Medicaid payments with cash requests of forty percent of expenditure amount for MCO premium payments.

### **Federal Draw Process**

#### *Draw Preparation*

There are four Fiscal Analyst 5's (FA5) within the Federal Financial Reporting section (Federal Claims unit, FFRU) who ensure HCA's draw amount is correctly calculated and based upon actual expenditures by reconciling expenditure and revenue reports from Enterprise Reporting for relevant cost objectives and revenue subsources for a given program.

For **weekly and bi-weekly** draws, the FA will run enterprise reporting year-to-date reports for the cost objectives (expenditures) and subsources (revenue) of a program/grant. The draw-down calculation is:

**Total Expenditures less Total Revenues.** This is performed for every cost objective/subsource for the specific grant. E.g. for Title XIX services, services for clients are coded with T3\*, D3\*, N3\*, and Q3\* cost objectives and subsources. Both enterprise reporting reports are saved into FFRU's shared drive for records.

For **premium** draws, the process is the same except for ProviderOne will send an email indicating how much the payment going out will be. The FA5 calculates 40% for the draw request so they have enough funds to cover the expenditure.

The FA5 will then login to the Grants Management System (GMS) and select the requesting grant. The FA5 uploads the ER reports and calculates the current and liquidation portions of the expenditures and revenue and difference to calculate the draw amount. These figures are entered into a summary tracking workbook for each grant located on the FFRU's shared drive for each draw. The FA5 will submit the draw request in GMS and sends screenshots of the draw preparation screens, e-mails from the other agencies for their draw portion, and draw calculation reports to Laura Roberts (primary approver) and Jill Arlow (backup approver) for approval of the draw calculation.

Laura/Jill will manually review the reports (assessment of the criteria used for the reports), current draw information, and backup history of the draws to ensure that the current draw was correctly calculated and based upon actual and liquidated expenditures and revenues to date.

### **Key Control #1 - Draw calculation and approval**

#### *Draw Process*

After approval, the FA5 will complete the draw process portion within GMS for the current draw. The FA5 will select the approved draw prep to include in the draw process and selects the correct agency, grant, and enters the appropriate draw amount per agency.

The FA5 will then log into the Federal Payment Management System (PMS), enter the Payee Account Number (C7133P1 for HCA; subaccount XIX-MAP3 is for tracking Title XIX assistance), select the correct subaccount, and enter the requested draw amount (all three requesting agencies). There is a screenshot of the draw confirmation included in the AFRS batch draw workbook.



## State of Washington

The FA5 will obtain a TM\$ draw workbook and prepare the draw information for a cash receipts journal, with the total draw amount split among the agencies, document number being used to process the revenues, and effective date of the deposit (next business day) and send it to HCA's Cash Management group to process an A-8 with the Treasury (created by a separate group/individual). Once this is processed, the Cash Management group will provide the FRRU a screenshot of the processed A-8 within TM\$ (included in the revenue recording workbook).

### **How Transactions are Recorded in AFRS:**

After the draw amount is approved and the actual draw is performed, a separate FA5 will prepare an AFRS batch to record the revenue via a AFRS toolbox upload. The FA will log into GMS and select the current draw and review the number of transactions, hash total, and JV total. GMS will generate the JV's toolbox upload sheet with the correct transaction codes, variable GLs, funds, revenue groups, and subrevenue codes for the current document number. The FA5 will review the transaction codings (001/003 for currents, 835/835R for liquidations), ensuring the correct amounts are present in total for each grouping. The FA will then upload the financial toolbox file and submit it to AFRS, comparing the hash and transaction number amounts to ensure the transactions uploaded correctly.

When the uploaded batch is cleared of errors, the overall draw/revenue workbook is loaded into GMS and the overall draw is saved. The FA will then send the draw workbook along with request for review and approval of the AFRS batch to Laura and Jill. Laura/Jill will review the transactions for accuracy by doing a side-by-side comparison in the workbook (amount, transaction codes, subsources) for final approval of the batch into AFRS and completion of the draw process within GMS (**Key Control #2 - AFRS batch approvals**).

### **Key Controls are as Follows:**

- **Key Control 1 (Rights & Obligations/Valuation)** - Fiscal analysts run expenditure and revenue reports and perform a reconciliation to calculate the correct request amount for Federal draw downs. This is submitted to the Federal Claim Supervisor for review of the calculations and reports prior to the actual draw.
- **Key Control 2 (Rights & Obligations/Valuation)** - After approval and submission of the draw, the FA5 will prepare the AFRS batch to record the revenue. This includes reviewing the sub-resource codes for the revenues, amounts to be recorded, and appropriate transaction codes (which will determine whether the transaction line will impact the GL1351 (for liquidations) or GL3210 (for current period amounts). The Federal Claims Supervisor will then review the draw workbook for accuracy and approve and release the batch into AFRS.

### **Noted Weaknesses are as Follows:**

None

### **D.5.PRG - Federal Grants in Aid**

# State of Washington

**Procedure Step:** Key Control #1 (Manual) - Draw Calculations and Approval

**Prepared By:** SRC, 8/13/2024

**Reviewed By:** RKM, 8/20/2024

## Purpose/Conclusion.

### **Purpose:**

To confirm the reconciliation of expenditures and revenues for the draw calculation (key control #1 for federal revenue draw downs) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy.

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude*

## State of Washington

*and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements.*

## State of Washington

*In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #1:** Draw Calculations and Approval

#### **Assertions:**

Rights and Obligations

Valuation

**Key Control #1** - Fiscal analysts run expenditure and revenue reports and perform a reconciliation to calculate the correct request amount for Federal draw downs. This is submitted to the Federal Claim Supervisor for review of the calculations and reports prior to the actual draw.

The understanding for this system is documented above in the "Controls - HCA" step.

### **1. Confirmation of Key Manual Control:**

## State of Washington

We reviewed current document FA0073 for the T19 Assistance 2024 weekly draw down revenue recording for the week of 2/05/24. The draw reconciliation was performed by Rossner Gideon, FA5. Included in the workbook were the two enterprise reporting reports used to calculate the draw amount. Relevant report criteria included:

- Expenditure report
  - Begin fiscal month - 01-Jul FY1
  - End fiscal month: Nov FY1
  - Cost objective: T4\*,D4\*,N4\*,Q4\*, [T44C\*,D44C\*,N44C\*,Q44C\*]
  - Cost allocation type: F
  - Expenditure content: Cash
  - Expenditure liquidation Content: All liquidations
- Revenue report
  - Begin fiscal month - 01-Jul FY1
  - End fiscal month: Nov FY1
  - Major source: 03
  - Source: 03/93
  - Subsource: 03/93/D4\*,03/93/T4\*,03/93/N4\*,03/93/Q4\*, [03/93/D44C\*,03/93/T44C\*,03/93/N44C\*,03/93/Q44C\*]
  - Revenue content: Cash
  - Revenue liquidation content: Yes

Cost objectives (Expenditures), as summarized:

- T\*\*\*:
  - Disbursements: 1,860,174,892.94
  - Liquidations: (136,817,662.55)
- D\*\*\*:
  - Disbursements: 907,638,005.39
  - Liquidations: (45,562,574.13)
- N\*\*\*: No activity
- Q\*\*\*: No activity

Revenue sub-sources (Revenues), as summarized:

- T\*\*\*:
  - Cash Receipts: 1,712,858,629.38
  - Liquidations: (137,626,213.55)
- D\*\*\*:
  - Cash Receipts: 907,851,661.12

## State of Washington

- Liquidations: (45,006,818.63)
- N\*\*\*: No activity
- Q\*\*\*: No activity

### Totals:

Expenditures to date: 2,585,432,661.65  
Revenues to date: 2,438,077,258.32  
Draw amount: 147,355,403.33

This total draw of **147,355,403.33** appeared as the HCA portion of the total draw (draws include amounts from DSHS and DCYF as the Medicaid grant is administered through HCA) for PMS Subaccount XIX-MAP24. The reports were submitted by Rossner Gideon, FA5, to Laura Roberts, Federal Claims Supervisor, for review on 2/05/24, at 9:00 am, and the draw was approved by Laura Roberts at 9:15 on the same day. The draw was then submitted by Chau Duong, FA5, at 10:15 am, and a Cash A8 Reciept was created by Diana Dunn, FA3, at 10:31 am. The total draw amount within the Federal Payment Management System totaled **207,010,820.61** (HCA's \$147M was part of the total draw, including DSHS and DCYF) was completed on 2/05/24 with a payment due date of 2/06/24 for Account Number C7133P1, subaccount XIX-MAP24. **No issues noted**

### Noted Weaknesses are as follows:

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.5.PRG - Federal Grants in Aid**

*Procedure Step:* Key Control #2 (Manual) - AFRS revenue recording and release

*Prepared By:* SRC, 8/19/2024

*Reviewed By:* RKM, 8/20/2024

## State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm the review and approval of the AFRS batching for revenues (key control #2 for federal draw downs) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

## State of Washington

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all*



## State of Washington

*control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #2** : AFRS Revenue Recording and Release

#### **Assertions:**

Rights and Obligations

Valuation

**Key Control #2** - After approval and submission of the draw, the FA will prepare the AFRS batch to record the revenue. This includes reviewing the sub-resource codes for the revenues, amounts to be recorded, and appropriate transaction codes (which will determine whether the transaction line will impact the GL1351 (for liquidations) or GL3210 (for current period amounts). The Federal Claims Supervisor will then review the draw workbook for accuracy and approve and release the batch into AFRS.

The understanding for this system is documented above in the "Controls - HCA" step.

#### **1. Confirmation of Key Manual Control:**

We reviewed current document FA0073 for the T19 Assistance 2024 weekly draw down revenue recording for the week of 2/05/24. The draw reconciliation was performed by Rossner Gideon, FA5.

To summarize the draw calculation:

Expenditures to date: \$2,585,432,661

Revenues to date: \$2,438,077,258

# State of Washington

Draw amount: \$147,355,403

The AFRS revenue batch included the A8 Form (AFRS Cash Receipts) which included portions for HCA, DSHS, DCYF.

The line calculations of the draw workbook for current year were recorded using TCs 001 and 003 as determined by either a debit or credit amount, totaling \$147,102,607

The line calculations of the draw workbook for liquidations were recorded using TC835 to adjust the receivable amount from the prior period, totaling \$252,796

For a total receipt amount of \$147,355,403.

The revenue recording workbook was prepared by Chau Duong, FA5, and approved by Laura Roberts, Federal Claims Supervisor, for batch HB 086.

## **Noted Weaknesses are as follows:**

- None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **D.5.PRG - Federal Grants in Aid**

*Procedure Step:* Controls - DSHS

*Prepared By:* SRC, 8/20/2024

*Reviewed By:* RKM, 8/22/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

# State of Washington

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in

# State of Washington

general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls for the Federal drawn down (DSHS) process address the following balance(s):

- **General Fund - Federal Grants in Aid**
- **Governmental Activities - Operating Grants and Contributions: Human Services**

Primarily Revenue Sources:

- Department of Agriculture (SNAP)
- Human Health Services (HHS) Medicaid

For the following assertions:

- **Rights and Obligations** - Federal draw-down requests may not be based on actual grant expenditures in accordance with federal cash management requirements.
- **Valuation** - Federal Grant draw-down requests may not be correctly calculated

## **Gain an Understanding of Internal Controls**

On July 23, 2024, we met with:

- Christine Johnson, Administrative Services Manager

## State of Washington

- Christina Choate, Program Services Manager (took over for Gwendolyn Dain in May 2024)
- Debra Trickler, Accounting and Internal Control Administrator (ESA)
- Julia Mosier, Office Chief (ALTSA/DDA)
- Rick Meyer, External Audit Compliance Manager
- Raiatea Arcuri, Senior Financial Coordinator
- Temeke Maxwell, Federal Accounting and Reporting Manager (ESA)
- Summer Garcia, Staff Services and Operations Consultant
- Rebecca Doane, Office Chief (OAS)

A high level summary of the draw process is as follows:

- DSHS Technology Services Division loads a report into the Grants Management System (GMS) with data from AFRS for the relevant Medicaid cost objectives and subsources for revenue, expenditures, and liquidations processed through the prior day. AFRS data is loaded into GMS to assist with calculating the draw amount using the following calculation: Total Revenue – Total Expenditures – Liquidations = draw or return amount showing in GMS.
- The Senior Financial Coordinator reviews the Title XIX Medicaid Assistance draws weekly on the first business day of the week and Administrative draws during 'payday draws,' the day before payday; if any special draws are necessary, they are created as needed.
- The Senior Financial Coordinator reviews the draw amount in GMS, the Administrative Services Manager or Program Services Manager approves the draw amount in GMS, and the Grant Specialist (a Fiscal Analyst) draws the funds within GMS, as well as processes the batch to record the revenue for the draw through AFRS. Within GMS each position verifies the data and checks a box in GMS to ensure accurate calculations, review and approvals are processed prior to finalizing each draw request.

### **Draw Frequency:**

Title XIX - Weekly, Monday by 9am

Payday - Bi-Weekly

### **Federal Draw Process**

#### *Pre-Draw*

**Nightly**, an AFRS report with the day's transactions (through the cost allocation system) is generated and sent to WaTech. WaTech sends the report to the DSHS IT department who review for federal caps and revenue related to cost objectives and revenue sources then, upload the relevant data into GMS where updated revenues and expenditures can both be accessed in the morning.

**The day before a draw**, the Senior Financial Coordinator (SFC) initiates a review through email to program staff in the field. The staff then performs a review in GMS and sends confirmation of the review to back to OAS (by clicking a button). The SFC will also check for funds that are expired or fully spent and communicate notes or any other issues in the GMA notes feature. On the ESA side, staff will run a LOC credit balance report and send it to the grant managers who will review the numbers and change or deny the draw as necessary.

# State of Washington

## *Creating the Draw Request*

The Senior Financial Coordinator initiates the draw requests by comparing the reported amounts within GMS to an AFRS report for revenue, expenditure, and liquidation data for the relevant subsources (revenue) and cost objectives (expenditures). The Senior Financial Coordinator reconciles the report calculation to the pending draw screen amounts in GMS to ensure that the draw amount is correctly calculated. When the draw amount is correct, the Senior Financial Coordinator signs off on the draw amount and sends the Administrative Services Manager and Program Services Manager an e-mail summarizing the total draw amount, with an attached report for HCA. The Administrative Services Manager/Program Services Manager will review the related AFRS reports and the amounts within GMS to ensure that the total revenues, expenditures, and liquidations were captured for the draw process. After approval, the draw is sent to Fiscal Analyst (FA) staff to process the draw, bring in the funds from PMS, and process the Journal Vouchers (JVs) **(Key Control #1 - Draw Calculation and Approval - Rights & Obligations/Valuation)**.

## *HCA Draw Process and Recording*

HCA is the administering agency for Medicaid; as such, HCA is issued the grant and LOC (Letter of Credit) authorization amount for Medicaid. HCA processes draw requests from DSHS and DCYF during the weekly, semi-monthly, and ad-hoc draw requests within the Federal Payment Management Services (PMS) system.

After receiving approval from the Administrative Services Manager/Program Services Manager for the draw amount, the Senior Financial Coordinator will send HCA an e-mail with the AFRS report used in the draw calculation, alongside the agency's approval. During this time, HCA will work with DSHS if there are any discrepancies or if the draw amount needs to be adjusted for any reason (e.g. HCA requests that DSHS only draws up to a certain amount because of LOC authorization). HCA staff will create the draw within PMS and begin their process of creating the cash receipt A8/TM\$ journal, as they receipt the actual grant reimbursements (in total) as well. The A-8 entry by HCA is split among the requesting agencies (DSHS, DCFY, OFM as applicable) and is sent by the HCA creator to the DSHS FSA/OAS GMS share box.

## **How Transactions are Recorded in AFRS:**

A Fiscal Analyst records payment transactions to AFRS using a journal voucher template. For each draw, the Fiscal Analyst will move the current document number generated by GMS to the reference document field and uses HCA's current document number to ensure that the reimbursement and JV match HCA's. GMS will generate the JV's toolbox upload sheet with the correct transaction codes, variable GLs, funds, revenue groups, and subrevenue codes for the current document number. The FA will review the transaction codings (001/003 for currents, 835/835R for liquidations), ensuring the correct amounts are present in total for each grouping. The FA will then upload the financial toolbox file and submit it to AFRS, comparing the hash and transaction number amounts to ensure the transactions uploaded correctly.

The Program Services Manager/Administrative Services Manager, will review the batch to ensure the correct accounting coding is present and all relevant backup information is present within the draw/revenue recording workbook for final approval of the batch into AFRS **(Key Control #2 - AFRS Batch Approvals - Valuation)**.

# State of Washington

## **Supporting documentation within the draw workbooks include:**

From HCA:

- Embedded e-mail from HCA detailing the draw amount
- Screenshot from PMS for the draw
- A-8/TM\$ screenshot of the A-8 entry and breakdown of agency

From DSHS:

- Screenshots within GMS showing the approved pending draw and draw preparer's information
- Screenshots of the toolbox upload
- FPS Data Entry Report (shows summary information of the LOC subaccount and amount)
- Grant Financial Status Report (shows the LOC, total grant award, and summary draw calculation information)
- Approval e-mails by the Program Services Manager/Administrative Services Manager
- AFRS report that the draw calculations were based upon
- Back-up screenshots for each federal agency

## **Key controls are as follows:**

- **Key Control #1 (Rights & Obligations/Valuation)** - The Senior Financial Coordinator initiates the draw requests by comparing a report from GMS to a WEBI report of AFRS data based on AFRS revenue, expenditures, and liquidations. The Senior Financial Coordinator reconciles both reports to the pending draw screen amounts in GMS to ensure the draw amount is accurate. The Administrative Services Manager or Program Services Manager completes a secondary review of draw requests in GMS to ensure AFRS reports detailing total revenues, expenditures, and liquidations captured match the draw request with an accurate calculation before approving the draw calculation.
- **Key Control #2- (Rights & Obligations/Valuation)** - After HCA provides the A-8/TM\$ information for the actual federal reimbursement through PMS, a Fiscal Analyst will prepare the AFRS batch JV with transaction information from the GMS upload sheet, which includes the transaction codes, revenue subsources, fund, and variable GL codes. The Fiscal Analyst will review the report to ensure the transaction detail is accurate and matches the A-8/TM\$ from HCA. The Fiscal Analyst will submit the batch into AFRS and the Program Services Manager/Administrative Services Manager will perform a secondary review for correct account coding and amount and that all required reports/screenshots are within the JV workbook before approving and releasing into AFRS.

## **Noted Weaknesses are as follows:**

None

## **D.5.PRGR - Federal Grants in Aid**



# State of Washington

**Procedure Step:** Key Control #1 (Manual) - Draw Calculations and Approval  
**Prepared By:** SRC, 8/20/2024  
**Reviewed By:** RKM, 8/22/2024

## Purpose/Conclusion:

### **Purpose:**

To confirm the reconciliation of revenues and expenditures for the federal draw calculations (key control #1 for Federal draw downs) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

## State of Washington

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it*

## State of Washington

*would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #1:** Draw Calculations and Approval

#### **Assertions:**

Rights and Obligations

Valuation

**Key Control #1** - The Senior Financial Coordinator initiates the draw requests by comparing a report from GMS to a WEBI report of AFRS data based on AFRS revenue, expenditures, and liquidations. The Senior Financial Coordinator reconciles both reports to the pending draw screen amounts in GMS to ensure the draw amount is accurate. The Administrative Services Manager or Program Services Manager completes a secondary review of draw requests in GMS to ensure AFRS reports detailing total revenues, expenditures, and liquidations captured match the draw request with an accurate calculation before approving the draw calculation.

# State of Washington

The understanding for this system is documented above in the "Controls - DSHS" step.

## **1. Confirmation of Key Manual Control:**

We reviewed current document FA0047 (batch KX 139) for the T19 Assisst weekly draw down revenue recording for the week of 11/20/2023. Included in the draw workbook was the draw report, prepared by Beverley Muncaster, Senior Financial Coordinator, sent to HCA for DSHS's portion of the weekly draw which contained (in summary, based upon draw calculations (Current) Expenditures - (Current) Revenues - Net Liquidations) for AFRS transaction dates 11/06/23 - 11/13/23:

D4\*

Net current = \$76,298,676.82  
Net liquidations = \$(1,582,080.32)  
Net draw = \$74,716,596.50

T4\*

Net current = \$3,437,130.21  
Net liquidations = \$(188,629.81)  
Net draw = \$3,248,500.40

N4\*

Net current = \$0  
Net liquidations = \$(1,724.50)  
Net draw = \$(1,724.50)

**GMS Information for agency 3000:** Title XIX ASSIST - HCA to date (federal grant number 5-2405WA5MAP, LOC C7133P1)

Cash Disbursement to date: \$494,559,678.54  
Revenue Drawn to date: \$416,596,306.14  
Draw Amount: \$77,963,372.40

Total Actual draw = \$77,963,372.40

The subsorce amounts and total draw amount of \$77,963,372.40 was submitted for approval via e-mail by Beverley Muncaster to Gwendolyn Dain, Program Services Administrator, on 11/20/2023, alongside the Webi query and draw amount to submit to HCA. Gwendolyn reviewed the reports and approved the draw amount. This amount was present with the same information within GMS in the Approved Pending Draws tab after

# State of Washington

approval by Gwendolyn as "approved." **No issues noted**

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **D.5.PRG - Federal Grants in Aid**

*Procedure Step:* Key Control #2 (Manual) - AFRS Revenue Recording and Release

*Prepared By:* SRC, 8/20/2024

*Reviewed By:* RKM, 8/22/2024

Purpose/Conclusion:

### **Purpose:**

To confirm the review and approval for federal revenue AFRS batching (key control #2 for Federal draw downs) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

## State of Washington

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

## State of Washington

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

**Key Control #2:** AFRS Revenue Recording and Release

**Assertion:**

Valuation

Rights and Obligations

**Key Control #2 - (Rights & Obligations/Valuation)** - After HCA provides the A-8/TM\$ information for the actual federal reimbursement through PMS, a Fiscal Analyst will prepare the AFRS batch JV with transaction information from the GMS upload sheet, which includes the transaction codes, revenue subsources, fund, and variable GL codes. The Fiscal Analyst will review the report to ensure the transaction detail is accurate and matches the A-8/TM\$ from HCA. The Fiscal Analyst will submit the batch into AFRS and the Program Services Manager/Administrative Services Manager will perform a secondary review for correct account coding and amount and that all required reports/screenshots are within the JV workbook before approving and releasing into AFRS.

The understanding for this system is documented above in the "Controls - DSHS" step.

**1. Confirmation of Key Manual Control:**

We reviewed current document FA0047 (batch HB 055) for the T19 Assist weekly draw down revenue recording for the week of 11/20/2023.

The draw amount calculated by Beverley Muncaster, Senior Financial Coordinator, was \$77,963,372.40. After approval of the draw calculation by DSHS (Gwendolyn Dain, Program Services Manager), Beverley sent the draw information (grant information including: LOC (C7133P1), total grant award and authorization, disbursements to date and revenue to date, the Webi report used to calculate the draw amount, and the e-mail chain for approvals for the draw calculation as noted above) to HCA and DSHS staff.

HCA employee Rossner Gideon, FA5, submitted the request for payment totaling \$109,232,118.98 (HCA: \$30,667,044.42 and DSHS: \$77,963,372.40, and DCYF:601,702.16) for the weekly draw. The generated A8 by Diana Dunn, Medical Assistance Specialist 3 (HCA), included the total \$77,963,372.40 for agency 3000 (HCA).

The draw workbook (KX 139) recording the revenues was prepared by Summaiya Khan, FA4; included in the workbook were approvals by Gwendolyn Dain for the draw calculations, summary screenshot of approved pending draws from GMS for the relevant LOC, screenshot within the Federal Grant Management System and HCA's A-8/TM\$ information all showing the total draw amount for DSHS of \$77,963,372.40.

Another tab was "Original Data" which is the system interface between GMS/PMS and creates a report by LOC, transaction code, fund, program



## State of Washington

index, revenue sources, and subrevenue sources, with the referenced GMS doc number. This amount matches the draw calculations per revenue source within the draw calculation section within GMS/PMS. This report drives the AFRS transaction records for the toolbox upload within the "KX 139" tab.

The line calculations of the draw workbook for current year were recorded using TCs 001 and 003 as determined by either a debit or credit amount, totaling \$75,941,264.94

The line calculations of the draw workbook for liquidations were recording using TC835 to adjust the receivable amount from the prior period, totaling \$2,022,107.46.

The workbook was prepared/submitted by Summaiya Khan and approved by Gwendolyn Dain.

### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.5.PRG - Federal Grants in Aid**

*Procedure Step:* Risk Assessment

*Prepared By:* SRC, 8/16/2024

*Reviewed By:* RKM, 10/29/2024

Purpose/Conclusion:
---------------------

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*
  - *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*
  - *Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*
  - *Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*
- *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*
  - *Are there substantial pressures or motivations to misstate the balance?*
- *Inherent Risk due to Misappropriation*
  - *Is the account balance or transaction class susceptible to sizable misappropriation?*
- *Inherent Risk due to Non-Compliance*

## State of Washington

- *Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*
- *Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*
- *Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

# State of Washington

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

## **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- Rights and Obligations – LOW
- Valuation – LOW

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

- **Federal Draw Downs** – Rights and Obligations and Valuation

**MAX** – We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

## State of Washington

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

- Valuation – **LOW**
- Rights and Obligations – **LOW**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

- We will review a sample of drawdown revenue recordings and their related expenditure and revenue reports to ensure that the draw amount was correctly calculated and recorded.
- We will review a sample of drawdowns and their related expenditure and revenue reports to ensure that the draw amounts were based upon actual program expenditures.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **D.5.PRG - Federal Grants in Aid**

*Procedure Step:* Substantive Test  
*Prepared By:* SRC, 10/22/2024  
*Reviewed By:* RKM, 10/29/2024

Purpose/Conclusion.\*

#### **Purpose:**

To determine whether the entity has legal authority to collect or the legal right to reported revenues.  
To determine whether revenues were reported at properly valued or calculated amounts.

#### **Conclusion:**

The entities had a legal authority to collect/the legal right to reported revenues based upon expenditures data. **No issues noted.**  
The revenues were reported at properly valued and calculated amounts. **No issues noted.**

# State of Washington

## Testing Strategy:

The following is a list of **considerations** for testing the rights and obligations assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

- Evaluate activities and approved rate or fee schedules (especially new activities or changed schedules) to verify that the entity has the legal right to collect or impose the revenue.
- Review support for selected revenues or revenue streams to verify that the entity has the legal right to the reported revenue.
- Determine whether revenues are properly recorded for amounts collected by another entity and that there is an appropriate receivable to them.
- Determine whether amounts collected by the entity for other governments are properly segregated and accounted for and that there is an appropriate payable to them.

### Revenues related to Joint Ventures or Other Arrangements

- Review forming documents and agreements to verify rights to any revenues generated by the venture.

### Property Taxes - see separate step

\*\*\*\*\*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### Calculation

- Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.
- For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.
- Review related-party transactions to determine whether revenue transactions were correctly calculated.

### Realizable Value

- Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.
- Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

## State of Washington

- Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### Estimation / Recognition

- Review calculation and support for assumptions of any estimated revenues.
- Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

### Property Tax Revenues - see separate step

Guidance/Criteria:

**Add the Guidance/Criteria for each relevant assertion from the TeamStore. You may also include other resources that you used for testing.**

Record of Work Done:

### Population Sourcing and Reconciliation

**HCA:** [Population Reconciliation] tab "107\_CG"

**DSHS:** [Population Reconciliation] tab "300\_CG"

We ran queries from the ACFR database for significant balances (Rollup fund FAA and IS Sort Code CG) for DSHS and HCA. We ran queries in Enterprise Reporting Web Intelligence which were filtered to match the results of the ACFR database to obtain transaction level detail for sampling. We reconciled the amounts by source and GL to the ACFR query with **no variances noted**. As the total population of the Webi queries' FGIA revenues reconciled to the ACFR database, we consider the transaction data to be complete.

### Sample Frames

**HCA:** [Population Reconciliation] tab "107\_Sample Frame"

**DSHS:** [Population Reconciliation] tab "300\_Sample Frame"

Based upon overall analysis of the revenue sources (SAO source within ACFR database queries) and subsources (within Webi queries), we determined that we obtained sufficient coverage limiting testing to Title XIX Medicaid subsources: D\*, N\*, T\* and U\*

We filtered the Webi transaction data for Medicaid sub-sources\* (D\*, N\*, T\* and U\*) and summarized the transactions by document number (representing revenue draws) for sample frames:

**HCA:** 87 current doc numbers, totaling \$8,886,311,074.

**DSHS:** 78 current doc numbers, totaling \$4,098,997,806.

# State of Washington

## **Sample Number and Selection**

Based upon the substantive testing FA small population tables, we randomly selected and identified:

**HCA:** 7 transactions, no individually significant items

**DSHS:** 6 transactions, no individually significant items

## **Substantive tests performed to meet the Valuation assertion:**

**HCA:** [\[HCA - FS Sampling\]](#)

**DSHS:** [\[DSHS - FS Sampling\]](#)

### Testing Procedures:

*Weekly and Payday (semi-monthly draws)*

For the selected draws, we reviewed biennium-to-date expenditure Enterprise Reporting reports and Liquidation WEBI report for the relevant cost objectives/subsources and re-calculated the draw amount (current expenditures less liquidations) to ensure that the draws and amounts recorded to GL3210 were correctly calculated.

*Premium Draws (HCA Only)*

Premium draws are based upon a calculation of 40% times the ProviderOne expenditures for the weekly payment cycle. These are made as-needed, but are typically drawn near the end of a month to cover managed care premium payments. We verified the ProviderOne expenditures via reports provided by CNSI agents (ProviderOne vendor) to HCA and confirmed they matched the draw amounts for the timeframe.

### Testing Results:

Revenue draws (GL3210) were correctly calculated based upon expenditures and revenues for their given cost objectives/subsources. **No issues noted.**

## **Substantive tests performed to meet the Rights & Obligations assertion:**

**HCA:** [\[HCA - FS Sampling\]](#)

**DSHS:** [\[DSHS - FS Sampling\]](#)

### Testing Procedures:

*Weekly and Payday (semi-monthly draws)*

For the selected draws, we reviewed biennium-to-date expenditure and revenue Enterprise Reporting reports related to Cost Objectives D4\*, T4\*, U4\*, and N4\*, as well as, WEBI reports provided by the client in the Draw Workbooks for each sample. We calculated the difference between the Expenditures and Revenues related to the Cost Objectives for each sample to ensure it matched the draw amount.

*Premium draws (HCA only):*



# State of Washington

For the selected draws, we used the ProviderOne Expenditure Draw Report to confirm that the funds drawn matched the reported expenditures.

## Testing Results:

Revenue draw amounts (GL3210) are correctly based upon actual cash expenditures (GL6510) for their respective subsources and cost objectives.

## D.6.PRG - Education

*Procedure Step:* Summary & Conclusion

*Prepared By:* NJH, 9/11/2024

*Reviewed By:* CJG, 11/18/2024

Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting*

## State of Washington

*the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in*

## State of Washington

*the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

#### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

#### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

### **D.6.PRG - Education**

*Procedure Step:* Understanding of Line Item

*Prepared By:* NJH, 6/10/2024

*Reviewed By:* RKM, 7/5/2024

# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.
- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or

## State of Washington

reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions:**

We reviewed the prior audit and did not note any exceptions relevant to these line items.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

- General Fund - Education

We met with Amy Harris, Director of Federal Fiscal Policy and Grants Management, Amy Kollar, Director of Agency Financial Services, and Rachel Patrick, Account General Manager, on 6/10/24 from OSPI to gain an understanding of the line item as well as ask about internal controls. They noted that there were no changes from the PY other than a minor staff change.

We gained an understanding of the composition of this ACFR line item through inquiry with OSPI staff and review of the PY AFRS database reports (ER) for FY23. Objects beginning with "N" comprised a majority of the education expenditures. These represent apportionment payments made to all of the schools in Washington State, labeled as "Other Grants & Benefits" which makes up roughly 96% of the entire line item balance. The OSPI Apportionment System is used for all apportionment expenditures. After reviewing the AFRS database reports (ER),

## State of Washington

budget documents, and the agency website, we did not identify any significant events or changes from last year that affect the line item or risks of misstatement.

Per PY, our approach for the reconciliations of governmental fund statements to the government wide statements is to rely on our substantiation of the governmental fund statements and governmental activities column and then to agree the reconciliation to these other substantiated statements.

### **(3) Updates to Significant Account Matrix:**

We identified no changes that need to be made to the Significant Account Matrix.

### **D.6.PRG - Education**

*Procedure Step:* Controls - Apportionment

*Prepared By:* NJH, 6/12/2024

*Reviewed By:* RKM, 8/6/2024

Purpose/Conclusion.:

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy.:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.

- In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
- Identify controls systems covering all relevant assertions for all significant classes of transactions.
- Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
- Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
- Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control

## State of Washington

- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**



# State of Washington

## Financial Statement Audits Planning Guide

Record of Work Done:

Internal controls in the Apportionment System address the following balance(s):

- Governmental Fund - Education

For the following assertions:

- Completeness: There is a risk that apportionment distributions omit or are less than source records. There is a risk of improper expense recognition resulting in understatement of apportionment distributions.

### **Gain an Understanding of Internal Controls**

We met with Amy Harris, Director of Federal Fiscal Policy and Grants Management, Amy Kollar, Director of Agency Financial Services, and Rachel Patrick, Accounting General Manager, on 6/10/24 from OSPI to gain an understanding of the line item as well as ask about internal controls. They noted that there were no changes from the PY other than a staff change. The staff change occurred 10 days prior to the meeting date. Jeannie Walker, the former Accounts Payable Supervisor, retired and Dereka Pedersen took over her duties with her title of Assistant General Accounting Manager.

Using the Senate Budgets and the Supplemental budgets, Washington State sets and updates the state appropriation for each fiscal year. The most recent budget, [2024 Supplemental Operating Budget](#), was passed March 7th, 2024. OSPI uses a portion of the appropriation to provide funding ("apportionment") to the schools in Washington State. This is noted in Part V Sec. 504 (pg. 683 of 896) of the passed budget showing the approved state appropriation for FY24 "General Apportionment" was \$9,784,078,000. Note here that this is only for "general apportionment" and does not include other state budgeted amounts granted to OSPI.

We met internally with Lauren Mason, IT Auditor (SAO), and Travis Jones, IT Auditor (SAO), on 6/12/24 to gain an understanding of how apportionments are calculated and paid for FY24 and to confirm that there were no changes from the prior year. We can rely on their understanding of apportionment as they are conducting a performance audit of OSPI in conjunction with our audit for FY24 and were in the process of confirming systems related to apportionment and have already met with OSPI staff recently. They confirmed that the following procedures are still in place related to how apportionment is calculated and paid:

### **How Apportionment is Calculated:**

# State of Washington

Apportionment amounts are determined by student enrollment and transportation. That enrollment data is submitted to OSPI from each school district with approval from their Educational Service District through the P223 system. Local education agencies (LEAs) complete forms P-223, P-223H, P-223S, or P-240 which includes data about their student enrollment. The enrollment data is then sent to Melissa Jarmon, Apportionment Payment Supervisor, to upload into the apportionment system. The apportionment system is a Education Data System (EDS) that compiles all of the data from the P-223, P-223H, P-223S, and P-240 forms. Transportation data is calculated through the Student Transportation Allocation Reporting System (STARS) with information provided from school districts.

The school year runs from September to August. From September to December, schools submit their estimated enrollment data to OSPI through form F-203 with approval from their Educational Service District. This data helps determine how much funding each school needs. Transportation funding will use last school year values until February when new data from STARS is available for the new school year. A true-up adjustment is made in January to reflect actual enrollment data. From January to the end of each school year, actual enrollment data is used to determine funding to the schools. Melissa enters the data from the district into the apportionment system.

## How Apportionment is Paid:

Payments are made through the following methods:

- **Office of the State Treasurer (OST):** Payments made through OST are determined by subtracting the amount of the warrant payments from the total amount of apportionment for the month. Fiscal Office at OSPI notifies OST using a Disbursements Request memo how much apportionment is to be distributed for the month to various Country Treasurers and Colleges. Once OST disburses the funds on the last working day of the month, the agency will send OSPI the report, "DetailReport 721," to confirm the disbursement.
- **Warrants:** Payments made through warrants normally comprise less than 1% of the apportionment to be paid for Month 1. On the Form 1198, they are highlighted in yellow and include: DSHS, the tribal agencies, charter schools, School for the Blind, Suquamish Tribal Education Department, WA State Center for Childhood Deafness and Hearing Loss, and the Washington Military Department.

The following controls are provided in the Apportionment Internal Control document [] received by OSPI staff. Note that we met with OSPI staff on 7/10/24 and were informed that their internal control document is outdated and lacks detailed processes that are in place. Rachel Patrick, Account General Manager, noted that she will be updating it this year. Therefore, the following controls are a combination of our understanding gained from discussion and walkthrough with OSPI staff as well as information in the original internal controls document.

## How Transactions are Recorded in AFRS:

The Fiscal Analyst records the payments in AFRS using the Financial Toolbox to prepare two separate batch's: one for OST payments and one for warrants. A batch is prepared for the Accounts Payable Supervisor's review, which includes:

- Upload report from the Financial Toolbox - Confirms that the data was uploaded to AFRS
- Distribution of Funds by Source memo
- Form 1198

## State of Washington

- Disbursements Request memo
- DetailReport 721

Before the batches are released in AFRS, the Accounts Payable Supervisor reviews the batches to ensure that the journal voucher is supported by the documentation noted above. At the beginning of the month, Dereka Pedersen, the Assistant General Accounting Manager, performs a monthly reconciliation using the Reconcile Apportionment Spreadsheet. She reviews the Distribution of Funds by Source memo against the actual AFRS distribution data (pulled from an AFRS query) to ensure that amounts are recognized in the proper period. **(Key Control #1 - Manual, Completeness)**. She also reviews the DetailReport 721 from the Office of State treasurer to AFRS distribution data for the month to ensure that the amount in AFRS represent all expenditures for the month.

### Monthly Monitoring of Appropriation vs. Expenditures

To verify that expenditures do not exceed appropriations each month, Amy Kollar, the Director of Agency Financial Services, reviews the EOY Apportionment Projections Summary Spreadsheet for any variances and discrepancies between the budgeted appropriations, the actual amount distributed for each month, and the remaining balance left for the year. **(Key Control #2 - Manual, Completeness)**. Every May, she will also use a spreadsheet to estimate June expenditures and total expenditures for the year to identify programs that have excess appropriation or are in shortfall to help plan for the upcoming year.

### Key Controls are as Follows:

- **Key Control #1** - At the beginning of the month, Dereka Pedersen, Assistant General Accounting Manager, performs a monthly reconciliation using the Reconcile Apportionment Spreadsheet. She reviews the Distribution of Funds by Source memo against the actual AFRS distribution data (pulled from an AFRS query) to ensure that amounts are recognized in the proper period **(Manual - Completeness)**.
- **Key Control #2** - Each month, Amy Kollar, Director of Agency Financial Services, reviews the EOY Apportionment Projections Summary Spreadsheet for any variances and discrepancies between the budgeted appropriations, the actual amount distributed for each month, and the remaining balance left for the year **(Manual - Completeness)**.

### Noted Weaknesses are as Follows:

- None

### D.6.PRG - Education

*Procedure Step:*      Key Control #1 (Manual)

# State of Washington

*Prepared By:* NJH, 7/12/2024

*Reviewed By:* RKM, 8/6/2024

Purpose/Conclusion:

**Purpose:**

To confirm at the beginning of the month, Dereka Pedersen, Assistant General Accounting Manager, performs a monthly reconciliation using the Reconcile Apportionment Spreadsheet. She reviews the Distribution of Funds by Source memo against the actual AFRS distribution data (pulled from an AFRS query) to ensure that amounts are recognized in the proper period (***Key Control #1 - Manual, Completeness***) in order to assess control risk

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

## State of Washington

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

## State of Washington

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #1 (Completeness):** At the beginning of the month, Dereka Pedersen, Assistant General Accounting Manager, performs a monthly reconciliation using the Reconcile Apportionment Spreadsheet. She reviews the Distribution of Funds by Source memo against the actual AFRS distribution data (pulled from an AFRS query) to ensure that amounts are recognized in the proper period.

The understanding for this system is documented above in the [[Controls - Apportionment](#)] step.

### **1. Confirmation of Key Manual Control:**

To confirm this key control we met with Dereka Pedersen, Assistant General Accounting Manager, on 7/8/24 to have her perform a walkthrough of the Reconcile Apportionment Spreadsheet for the month of April 2024. Additionally, we received a copy of this spreadsheet from Dereka on 7/9/24 and inspected the contents she reviewed with us during our meeting. For April, Dereka stated that after an apportionment batch is released in AFRS by the fiscal analyst team, at the start of the month of May she will open up the Reconcile Apportionment Spreadsheet and in the tab titled "Apr 2024 AFRS" will pull in AFRS data from GL 6505 - Accrued Expenditures/Expenses & GL 6510 - Cash Expenditures/Expenses for

## State of Washington

the month of April. On a separate tab titled "Apr 2024" she will pull in the details from the "Distribution of Funds by Source Memo" acquired from the Apportionment team after they confirm apportionments for that month to be released and sent over to OST. At the bottom of this tab she will reconcile the amounts from the memo and the AFRS data to look for any variances. For April she showed us that there was one variance for April for \$188,652.81 that was noted in her document as "Charter School Commission - not included in JV". ***No issues noted.***

There are two additional tabs in her document that Dereka mentioned in our walkthrough that we were able to confirm by inspecting the spreadsheet. One of these tabs is titled "Comparison to App" which shows all accounts in the general fund for each fiscal month. There is a running FYTD total that she will check against what is in AFRS at the time of this reconciliation. The total FYTD activity was \$13,304,546,289.54 and the amount in AFRS showed \$13,305,296,924.62 with a variance of \$143,590.01. Dereka did not explicitly address this variance in our walkthrough but through our inspection we were able to identify that this is coming from a timing issue of an amount corrected in May as well as a "suspense" payment yet to be disbursed. The other tab in this spreadsheet is titled "251 Rec Summary" which shows all of the months throughout FY24. Dereka added arrows and references for us to better understand where certain amounts are coming from throughout the spreadsheet. We were able to understand that the purpose of this tab is to show the activity for April (in this case) and the amount in recorded in AFRS as well as the total YTD total in AFRS for apportionment. There appeared to be no differences or variances noted here on this tab. ***No issues noted.***

### **Noted Weaknesses are as follows:**

- **None**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.6.PRG - Education**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* NJH, 7/12/2024

*Reviewed By:* RKM, 8/6/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm each month, Amy Kollar, Director of Agency Financial Services, reviews the EOY Apportionment Projections Summary Spreadsheet for any variances and discrepancies between the budgeted appropriations, the actual amount distributed for each month, and the remaining balance left for the year (**Key Control #2 - Manual, Completeness**) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated"*



## State of Washington

*step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider

## State of Washington

*whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #2 (Completeness):** Each month, Amy Kollar, Director of Agency Financial Services, reviews the EOY Apportionment Projections Summary Spreadsheet for any variances and discrepancies between the budgeted appropriations, the actual amount distributed for each month, and the remaining balance left for the year.

The understanding for this system is documented above in the [\[Controls - Apportionment\]](#) step.

### **1. Confirmation of Key Manual Control:**

To confirm this key control we met with Amy Kollar, Director of Agency Financial Services, on 7/8/24 to have her perform a walkthrough of the *EOY Apportionment Projections Summary Spreadsheet* for the month of April 2024. Additionally, we received a copy of this spreadsheet from Amy on 7/10/24 and inspected the contents she reviewed with us during our meeting. For April, Amy stated that this process will usually take place after the apportionment batch is released in AFRS by the fiscal analyst team, and after Dereka Pedersen, Assistant General Accounting Manager, has performed her reconciliation and variance check as identified at [\[Key Control #1 \(Manual\)\]](#). Amy noted that this spreadsheet consists of AFRS data for the particular month she is reviewing (in this case it was April 2024) compared to the total OSPI appropriation budgeted amount. Through Amy's walkthrough and inspection of the spreadsheet we were able to confirm this control as described in the following paragraph. **No**

# State of Washington

## *issues noted.*

The data is represented by legislative "sections" (i.e. 506 School Employee Compensation, 508 Transportation, etc.) as listed in the actual WA annual budget and is compared (in order from left to right) as Appropriations, the current month ending balance Amy is reviewing from AFRS, the remaining yearly balance, the projected budget left after the current month's apportionments, and the "final balance" to show any variances. For the fiscal year there was a budgeted appropriation of \$9,071,125,000 for section 504 (which included General Apportionment). At the end of April, AFRS showed an ending balance of \$8,892,279,301. Note here that we compared this ending balance amount with the amount on Dereka's *Reconcile Apportionment Spreadsheet* and found a slight variance of \$1,567 which we were able to identify as April substitute reimbursements from Amy's spreadsheet. ***No issues noted.***

## **Noted Weaknesses are as follows:**

- **None**

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **D.6.PRG - Education**

*Procedure Step:* Risk Assessment

*Prepared By:* NJH, 10/7/2024

*Reviewed By:* RKM, 10/14/2024

Purpose/Conclusion.\*

## **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*
  - *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*
  - *Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*
  - *Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*
- *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*
  - *Are there substantial pressures or motivations to misstate the balance?*
- *Inherent Risk due to Misappropriation*
  - *Is the account balance or transaction class susceptible to sizable misappropriation?*
- *Inherent Risk due to Non-Compliance*

## State of Washington

- *Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*
- *Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*
- *Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

# State of Washington

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- Completeness - **Low**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

- **Apportionment** – Completeness

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant

## State of Washington

class of transactions:

- Completeness - **Low**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

- For **Completeness**: We will review the monthly reconciliations between OST's FY24 distributed amounts to the amount reported in AFRS to determine whether all expenditures incurred during the period were reported. Additionally, we will determine if expenditures exceeded allocations at fiscal year end. We will verify that the amounts paid out to each school district through the Office of the State Treasurer (OST) represent all obligations incurred during the period and were supported by documentation, including form Report 1198 and a letter to OST. We will reconcile the "Grand Total" from the OST Distribution Detail 721 Report to the "Statewide Total" on the OSPI reports (Form 1198, apportionment memo and letter to OST) and review the apportionment memo, reconciliation worksheet, and other documentation to determine the amount of apportionment expenditures that occurred in FY24.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **D.6.PRG - Education**

*Procedure Step:* Substantive Test  
*Prepared By:* NJH, 10/7/2024  
*Reviewed By:* RKM, 10/14/2024

Purpose/Conclusion.
---------------------

#### **Purpose:**

To determine whether all expenses/expenditures incurred during the period were reported.

#### **Conclusion:**

We determined that all expenses/expenditures incurred during the period were reported. *No issues noted.*

# State of Washington

## Testing Strategy:

### **Completeness:**

The following is a list of **considerations** for testing the completeness assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Detail Roll-Up**

- Compare totals from general ledger to accounts payable, payroll or other subsidiary software modules.
- Review the government's reconciliation of general ledger to subsidiary systems.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

### **Cut off / Improper Expense Recognition**

- Scan expenditures recorded 1-3 months before and/or after fiscal year end (expenditures not charged to the current period). Based on the scan, test selected or sampled expenditures to determine if the expense should have been reported in the current period.
- Inquire with AP clerks regarding invoices held, but not entered as of year-end (ie: due to pending litigation or disputes).

### **Unrecorded Expenses**

- If the entity reconciles recorded revenues and expenses to bank activity, then reviewing monthly reconciliations and evaluating or testing reconciling items.

### **Accounts Payable**

- If entity uses a warrant clearing account for vendor payments, review the entity's year-end reconciliation of recorded vendor payments with disbursements from the clearing account.
- Review edit check reports from the AP system that might indicate missing payments.

### **Payroll**

- If entity uses a payroll clearing account, review the entity's year-end reconciliation of recorded payroll with disbursements from the payroll clearing account.
- Perform an expected payroll test by taking the prior audited payroll amount and adjusting it for expected changes.

*The analysis should consider changes in employees, COLA increases, salary scale increases if automatic, changes wages or benefits due to changes in policy or union negotiations changes, etc. Sources for these expectations should be obtained apart from the payroll records*



## State of Washington

*that are being tested. Since the auditor would not expect to be able to precisely predict payroll, the auditor should document a reasonable range within which actual payroll is expected to vary from the auditor's prediction.*

- If the board directly approves salaries for a significant amount of employees, verify whether the actual salaries for these employees is within an expected reasonable range of the approved salary.
- For small entities, compare payroll by employee to known employees per observation, organization charts or a phone list.
- Review edit check reports from the payroll system that might indicate missing payments.

### **Unrecorded Liabilities**

- Evaluate liabilities directly related to expenses for completeness. See the completeness steps for current and non-current liabilities for testing considerations.

*For example, if the entity reports a self-insurance liability, the auditor might evaluate whether the change in the liability (and related expense) was determined and recorded. If no liability was reported, then the auditor might determine whether such a liability (and associated expense) should have been reported.*

**OPEB** - auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

### **Removing Expenses from Accounting Records**

- Search for manual journal entries that credit (decrease) expenditures. Consider testing selected transactions.
- Identify transactions that void, cancel, or manually adjust transactions in subsidiary AP or payroll systems. Auditors may conclude that the total amount of such transactions are trivial or otherwise reasonably small. Or auditors may sample or select transactions for testing.

*Also see considerations under the "Not recording expenses" section.*

### **Interfund Expenses**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

Guidance/Criteria:

### **AUDIT CRITERIA - Occurrence**

## State of Washington

Key criteria that auditors will likely use when testing this area.

### **BARS [3.8.6](#) Use of Payroll and Claims Funds**

#### **AUDIT CRITERIA - Completeness**

Key criteria that auditors will likely use when testing this area.

**BARS [3.6.13](#) Utility Tax (*applies only to cities*)** - should be accounted for as a revenue in the general fund (3164000) and expenditure in the utility fund (53P0040), if the utility passes the tax on to its customers then the additional charges should be recognized as revenue (343P000) directly in the utility fund not in the general fund

### **BARS [3.8.6](#) Use of Payroll and Claims Funds**

Record of Work Done.

#### **Substantive tests performed to meet the Completeness assertion:**

See testing performed at [\[OSPI Testing\]](#).

We performed substantive testing to meet the completeness assertion by the following two testing methodologies described:

- OSPI provided us with various treasury reports and letters that include details about the net amount of apportionment to be paid out for each fiscal month throughout the FY24 year. We first analyzed and compared the apportionment amount shown on the letter sent to OST for funds disbursement with the amount shown on the "DistDetail721" report. We noted no variances between these reports. Additionally, we compared the internal OSPI apportionment "Report 1198" showing the distribution of state funds, the Type 9 payments, and amounts to state agencies & charters with the amounts reported to the state treasury. We noted no variances between the OSPI reports and the OST letters. We included July 2024 (FY 25) in the scope of our testing due to the frequency by which remaining PY funds are oftentimes paid out during the first few months of the next fiscal year. We noted variances for either the OST reports or the OSPI apportionment reports for July of FY25.

We determined that reported expenditures were complete for all periods evaluated. *No issues noted.*

- Additionally, we obtained the "June Items" excel workbook from Dereka Pedersen, Assistant General Accounting Manager, on 8/14/24 containing the total FY 24 OSPI reports, OST reports, AFRS JV log, and the reconciling apportionment spreadsheet, all in one workbook. We ran an Enterprise Reporting (ER) report for "GL Activity Flexible", for Fund 001, Object N, and GL account 6510 to obtain all of the grant/apportionment payments made throughout the year. We then sorted this report by fiscal month to determine the total

## State of Washington

apportionment paid out in AFRS. We compared these figures with the "AFRS Dist. JV & Detail Tranx Log" spreadsheet (included in the *June Items* workbook) which showed the total amount to be reported to OST and any necessary JV's needed for AFRS. We made two comparisons with these amounts: the first was comparing the AFRS Dist. Detail to our *Existence* testing OSPI Report 1198, where we noted no variances. We then compared the AFRS Dist Detail to the amounts reported on the ER Report, where we noted 4 months with variances. We inquired about these variances and determined that they are PY apportionments paid out during the current FY. As noted similarly above, we included July 2024 (FY 25) in the scope of our testing due to the frequency by which remaining PY funds are oftentimes paid out during the first few months of the next fiscal year. We expected to see a variance for July FY25 to include some FY24 apportionment amounts and we were able to confirm this by noting 12 transactions that had PY task codes for FY24 during July. From FY24 months, there were 18 total transactions that had PY task codes, resulting in 30 total PY transactions identified during our testing. To ensure all transactions were accounted for, we compared the total monthly AFRS Dist Detail with the total ER subtotal for all 13 months (including July of FY25), as well as the apportionments made in PY's, and confirmed that they tied to the ER Report subtotal of \$18,352,573,363.

We determined that all expenditures incurred during the period were reported. *No issues noted.*

### D.7.PRG - Due From Other Governments

*Procedure Step:* Summary & Conclusion  
*Prepared By:* EZM, 11/21/2024  
*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion.:

#### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

#### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

Testing Strategy.:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

# State of Washington

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?

## State of Washington

- If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
- If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

### **SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

#### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

#### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

## State of Washington

### Issues

ISS.1 - E: HCA_Receivables Lack of Complete Reconciliation Pay1 to AFRS		
<i>Prepared By:</i>	MRF, 10/17/2024	<i>Issue</i>  The Health Care Authority did not fully reconcile the fiscal year 2024 Due From Other Governments balance for PEBB and SEBB from PAY1 to AFRS. AFRS reported \$9,382,356 less than amounts included in PAY1 receivable reports.  We recommend the Health Care Authority improve resources (PAY1 reports, databases, etc.) to facilitate the tracking of invoices, payments, any related adjustments, and batched revenue transactions between PAY1 and AFRS.
<i>Reviewed By:</i>	CJG, 11/6/2024	
<i>Type:</i>	Financial Statements	
<i>Category:</i>	Accounting/Financial Reporting	
<i>Reporting Level(s):</i>	Exit Item	
<i>Impact</i>		
<i>Cost Savings:</i>		
<i>Questioned Costs:</i>	\$0.00	
NOTES		
<p>As part of the fiscal year 2021 ACFR, we noted HCA was not reconciling PAY1 Accounts Receivables to AFRS to ensure sub-ledger system information was reported accurately. We recommended the agency improve resources (PAY1 reports, databases, etc.) to facilitate the tracking of invoices, payments, any related adjustments, and batched revenue transactions between PAY1 and AFRS. As of fiscal year 2024, the agency has not implemented SAO's recommendation.</p> <p>We communicated this general issue to Rita Homan during our control meeting on 05/02/2024 and also to Will Sogge, External Audit Liaison on 09/13/2024 via Teams.</p> <p>See Level of Reporting Summary at: <a href="#">[LOR Summary]</a>. See the Aggregation of Misstatements: <a href="#">[Aggregation of Misstatements (GAAP)]</a>.</p>		
ISS.2 - V: HCA_Accounts Payable Reconciliations Were Not Performed Timely		
<i>Prepared By:</i>	EZM, 10/18/2024	<i>Issue</i>

## State of Washington

<i>Reviewed By:</i> CJG, 10/24/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Other <i>Reporting Level(s):</i>  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<p>The Health Care Authority did not prepare or review accounts payable reconciliations for PEBB and SEBB in a timely manner. These reconciliations are supposed to be performed at the end of each month, but the PEBB reconciliation for the month of November 2023 wasn't prepared or reviewed until January 2024 and the SEBB reconciliation for the month of November 2023 wasn't performed until March 2024.</p> <p>We recommend the Health Care Authority prepare and review accounts payable reconciliations at the end of each month.</p>
---	--

### NOTES

LOR Summary: [[LOR Summary](#)]

Communication: We communicated this issue to Rita Homan, Deputy Accounting Section Manager on October 17, 2024.

### ISS.3 - E: HCA\_Non-Confidential Provider One IT Controls

<i>Prepared By:</i> DLE, 10/17/2024 <i>Reviewed By:</i> CJG, 11/6/2024 <i>Type:</i> Financial Statements <i>Category:</i> IT Controls - Non-Confidential <i>Reporting Level(s):</i> Exit Item  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<p><i>Issue</i></p> <p>The Health Care Authority did not document procedures for performing rate changes in ProviderOne.</p> <p>We recommend the Health Care Authority document procedures for performing rate changes in ProviderOne.</p>
---	--

## State of Washington

### NOTES

**Communication of the Audit Issue with the Client:**

We verbally communicated the issue to Kari Summerour, External Audit Liaison, Dineen Kilmer, ProviderOne Section Manager, Ed Hicks, IT System Admin, and Angie Skinner IT System Admin, in a Teams meeting on 10/11/2024.

### ISS.4 - V: HCA\_Confidential IT Controls\_SOC Audit (Part of ML)

*Prepared By:* DLE, 10/17/2024  
*Reviewed By:* SHW, 12/9/2024  
*Type:* Verbal Recommendation  
*Category:* IT Controls - Confidential  
*Reporting Level(s):*

*Impact**Cost Savings:**Questioned Costs:* \$0.00*Issue*

We identified the following weaknesses related to the Acentra Health, LLC Provider One SOC 2 Type 2 audit:

The ProviderOne vendor's SOC 2 Type 2 audit did not cover the entire fiscal year 2024. The audit did not include the first six months of the fiscal year, July 1, 2023 - December 31, 2023.

The Authority receives and reviews the Acentra Health ProviderOne SOC 2 Type 2 audit report to determine whether there are exceptions that require corrective action. However, there are no documented procedures for receiving and reviewing the report to ensure the review is adequately and consistently performed.

The Authority did not maintain documentation to support there was a review of the SOC 2 Type 2 audit report.

We recommend the Authority:

Continue to work with its vendor to obtain an annual SOC 2 Type 2 report that covers the entire fiscal year.

Implement formal procedures for receiving and reviewing the report to include maintaining documentation evidencing the review occurred and the results.

### NOTES

**Level of Reporting Summary:** [LOR Summary].

**INCLUDED IN ML at Iss.40**



## State of Washington

### Communication of the Audit Issue with the Client:

We verbally communicated the issue to Kari Summerour, External Audit Liaison, Dineen Kilmer, ProviderOne Section Manager, Ed Hicks, IT System Admin, and Angie Skinner IT System Admin, in a Teams meeting on 10/11/2024.

### Rational for Level of Reporting:

We issued a Management Letter in FY20 as HCA did not obtain a SOC report that covered any part of the fiscal year. In prior audits we issued Management Letters when HCA obtained SOC reports that covered only six months of the fiscal year. Although we did not identify material errors, from a qualitative standpoint there is a possibility of additional undetected misstatements. To date HCA has been unable to obtain funding from the Legislature to pay for annual service organization reports.

### Issue history:

FY23 Finding (No report)  
FY22 Management Letter (Report covered 6 months)  
FY21 Finding (No report)  
FY20 Management Letter (Report covered 6 months)  
FY19 Finding (No report)  
FY18 Management Letter (Report covered 6 months)  
FY17 Finding (No report)  
FY16 Management Letter (Report covered 6 months)  
FY15 Finding (No report)  
FY14 Management Letter (Report covered 3 months)  
FY13 Finding (No report)

### ISS.6 - E: WSDOT\_Depreciable Assets Manual Input Error

<i>Prepared By:</i>	NJH, 7/11/2024	<i>Issue</i>
<i>Reviewed By:</i>	RKM, 12/17/2024	The Department of Transportation did not ensure the monthly depreciation amount and the total accumulated depreciation were correct for a selected asset in the Computer Aided Facilities Management (CAFM) system. There were approximately five months of missing depreciation, which was due to manual input error of the placed-in-service date.
<i>Type:</i>	Financial Statements	
<i>Category:</i>	Accounting/Financial Reporting	
		We recommend the Department of Transportation have the Capital Facilities

## State of Washington

<p><i>Reporting Level(s):</i> Exit Item</p> <p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i> \$0.00</p>	<p>Financial Manager frequently (once a month or other periodic interval) review the manual inputs of required CAFM fields such as the "Date Acquired" and the "Date Placed in Service" to ensure they are appropriate as they relate to the original work order or the completed work timeline.</p>
<b>NOTES</b>	
<p><b>See Level of Reporting Summary at: <a href="#">[LOR Summary]</a>.</b></p> <p><b>Communication of the Audit Issue with the Client:</b></p> <p>We verbally addressed this issue during a meeting with Elena Fehr, Facilities Inventory Specialist, and Krystle Mize, DOT Budget &amp; Financial Manager, on 6/27/24 and sent over a copy of our recalculation that led us to discover the error. Elena Fehr confirmed through screenshots &amp; email that she had forgotten to update the system with the correct date acquired, which was causing the CAFM system to calculate straight-line depreciation incorrectly. She successfully updated the CAFM system with the corrected "date acquired" field and depreciation amounts. We were able to verify this correction on our end.</p>	
<b>ISS.8 - E: ESD_PFML Control Weaknesses</b>	
<p><i>Prepared By:</i> JLE, 10/17/2024</p> <p><i>Reviewed By:</i> RKM, 12/17/2024</p> <p><i>Type:</i> Financial Statements</p> <p><i>Category:</i> Accounting/Financial Reporting</p> <p><i>Reporting Level(s):</i> Exit Item</p> <p><i>Impact</i></p>	<p><i>Issue</i></p> <p>The Employment Security Department has the following control weaknesses in its Paid Family and Medical Leave (PFML) program:</p> <ul style="list-style-type: none"> <li>Claim adjudicators have the ability to manually adjust/override system-calculated benefit amounts; there is no secondary review performed over such manual adjustments.</li> <li>The Employment Security Department has not implemented detective controls to identify multiple payments made to a single claimant between the PFML and workers' compensation benefit programs.</li> <li>The Employment Security Department does not maintain documentation related to its weekly cross-match of OMAC Portal and NGTS</li> </ul>

# State of Washington

<p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i>     \$0.00</p>	<p>unemployment data, for purposes of identifying employers who may be liable for PFML premium assessment.</p> <p>We recommend the Employment Security Department review all manual adjustments to benefit claims, implement detective controls to identify unallowable "double dipping" of PFML and workers' compensation benefits, and maintain documentation related to its weekly cross-match activities.</p>
<p><b>NOTES</b></p>	
<p>We communicated these issues to Stephanie Esekzen (External Audit Liaison) on 5/16/2024, 5/30/2024, and 7/9/2024.</p>	

## ISS.9 - V: Seattle Colleges\_Lack of Documentation for General IT Control

<p><i>Prepared By:</i> MRF, 10/17/2024</p> <p><i>Reviewed By:</i> CJG, 10/24/2024</p> <p><i>Type:</i> Verbal Recommendation</p> <p><i>Category:</i> Accounting/Financial Reporting</p> <p><i>Reporting Level(s):</i></p>	<p><i>Issue</i></p> <p>Seattle Colleges performs a review of rate table updates for state SBCTC tuition rates and the College's term rate adjustments, but does not document it.</p> <p>We recommend Seattle Colleges retain documentation specific to this process.</p>
<p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i></p>	

### ISS.10 - E: OST Investment Fair Value Excludes Interest

<p><i>Prepared By:</i> SHW, 10/16/2024</p> <p><i>Reviewed By:</i> RKM, 12/17/2024</p> <p><i>Type:</i> Financial Statements</p>	<p><i>Issue</i></p> <p>The State Treasurer's Office did not report all June interest earned as part of the June 30, 2024, par and fair value of investments held in bank accounts. The</p>
--	--

## State of Washington

<i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Exit Item  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<p>interest earned, totaling \$35,378,092, was reported as interest receivable rather than cash and investments.</p> <p>We recommend the Treasurer and OFM include interest earned and received in June as part of cash and investments reported at fiscal year-end.</p>
---	--

### NOTES

**See Level of Reporting Summary at:** [LOR Summary](#)

**Communication of the Audit Issue with the Client:**

We notified Heidi Algieri and Devon Phelps about the issue on 10/16/24

### ISS.11 - E: HCA\_Misstatement of Due From Other Governments Receivables

<i>Prepared By:</i> MRF, 10/22/2024 <i>Reviewed By:</i> RKM, 11/8/2024 <i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Exit Item  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<p><i>Issue</i></p> <p>The Health Care Authority incorrectly excludes payments for the current month if the payments are received after billing is generated for the next month in the Pay1 system. The system did not include some payments in the calculation of the Due From Other Government's receivable balance as of June 30th, 2024. The omissions overstated the balance by the \$15,456,165 payment amounts and also overstated premium and assessment revenue by the same amount as of June 30th.</p> <p>We recommend the Health Care Authority update the Pay1 system so that it records payments in the month received.</p>
---	--

### NOTES

## State of Washington

We communicated the known issue over Teams with Rita Homan on 09/18/2024, and communicated the projected misstatement via email same day, and included William Sogge and Kari Summerour (HCA's external audit liaisons). Rita Homan provided additional documentation to show the true misstatement of the line item, which we reviewed and agreed with. We communicated our acceptance of the known misstatement of 15.5M on 10/16/2024 via email. See LOR here [[LOR Summary](#)] and AOM here [[Aggregation of Misstatements \(GAAP\)](#)].

### ISS.12 - V: ECY\_Application of Loan Payments

<i>Prepared By:</i> EJB, 10/22/2024 <i>Reviewed By:</i> CJG, 11/6/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<i>Issue</i> The Department of Ecology did not ensure Clean Water State Revolving Fund loan payments were applied correctly. The payments in November on three loans were incorrectly applied to only one loan. The selected loan was understated by \$59,250. However, this error does not effect the overall amount reported as due from other governments.  We recommend the Department of Ecology review their reconciliation process of eHub receivables on a loan by loan basis before entry into AFRS.
--	--

### NOTES

**See Level of Reporting Summary at:** [[LOR Summary](#)].

#### **Communication of the Audit Issue with the Client:**

We emailed Beth Swanson, Senior Financial Advisor, on 10/22/2024 informing her that "We have finished the testing for the loans receivable line item on the ACFR. When we take into consideration the one issue I ran into that I had emailed you about earlier this week, this misstatement was \$59,250 for the one loan. However, in the aggregate, there is minimal affect. We recommend that ECY does a loan by loan reconciliation before making an entry into AFRS."

We note that as of 10/4/2024, it would be too late to make a correcting entry into AFRS. Therefore, this misstatement will remain uncorrected.

## State of Washington

### ISS.13 - V: CCS\_Lack of Documented Review and Approval of Investment Reconciliations

<i>Prepared By:</i> JAG, 10/14/2024 <i>Reviewed By:</i> RKM, 11/8/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>     <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<i>Issue</i> The Community Colleges of Spokane did not evidence review and approval of their June 2024 bank reconciliations for investments.  We recommend the Community Colleges of Spokane include a signature and date of review on their investment reconciliations to evidence that the review and approval has taken place.
--	--

### NOTES

See LOR summary here: [LOR Summary](#)

We communicated this issue to Tiffany Henderson, Director of Financial Reporting on 10/14/2024.

### ISS.14 - V: Seattle Colleges\_Complete and Timely Cash Reconciliations

<i>Prepared By:</i> MRF, 10/17/2024 <i>Reviewed By:</i> CJG, 11/6/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>	<i>Issue</i> Seattle Colleges did not complete reconciliations of cash balances in a timely manner. They performed a year end physical cash count, but had not reconciled to the GL.  We recommend Seattle Colleges promptly reconcile cash accounts with agency records on a monthly basis, as required by SAAM 85.50.40.c.
--	---

## State of Washington

<i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	
--	--

### NOTES

We communicated this issue to David Williams, Director of Financial Reporting, and Charlene Rios, Director of Accounting on October 14th, 2024 via Teams in the weekly checkin.  
See LOR here [[LOR Summary](#)].

### ISS.15 - E: ESD\_Misstatement of NGTS Deposits Reporting to AFRS

<i>Prepared By:</i> CJM, 10/17/2024 <i>Reviewed By:</i> RKM, 12/17/2024 <i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Exit Item  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	<i>Issue</i> The Employment Security Department was unable to reconcile two of the 24 NGTS deposits we tested to the bank statements. The variances, totaling \$122,737, projected into the population resulting in a likely misstatement of \$1,635,945. Upon further review, the Department determined NGTS had double posted a bank deposit when the bank had only received one.  We recommend the Department verify the number of NGTS deposit postings match the number of bank deposits to ensure deposits can be reconciled to the bank statements and cash and revenues are accurately reported.
---	---

### NOTES

LOR: [[LOR Summary](#)]  
We communicated this issue to Stephanie Eskesen, Audit Liason on October 10, 2024.

### ISS.16 - E: ESD\_UTAB Allowance Calculation Error

<i>Prepared By:</i> DRR, 10/23/2024 <i>Reviewed By:</i> CJG, 11/6/2024	<i>Issue</i> The Employment Security Department did not thoroughly review their calculation
---	--



## State of Washington

<i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Exit Item  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	<p>of the UTAB allowance for doubtful receivables to ensure that it was correct. This error resulted in an overstatement of the allowance for uncollectible receivables by \$17,106,288 and an equal understatement of other receivables.</p> <p>We recommend the Employment Security Department thoroughly review their allowance calculations to ensure the calculation is accurate.</p>
---	--

### NOTES

We communicated this error to Meghan Phelps, Treasury Manager, Ibrahim Dembele, Treasury Director, Stephanie Eskesen, Audit Liaison, and Jay Summers, Audit Director on October 10, 2024.

LOR: [\[LOR Summary\]](#)

### ISS.17 - E: ESD\_Certified Uncollectible Amount

<i>Prepared By:</i> DRR, 10/23/2024 <i>Reviewed By:</i> CJG, 1/8/2025 <i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Exit Item  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<p><i>Issue</i></p> <p>The Employment Security Department used incomplete data as the basis for its certified uncollectible amount (CUA). The CUA is used to calculate the NGTS allowance. From 2018 to 2021 and 2024 the CUA was significantly higher than in 2022 and 2023. There is a potential allowance understatement of \$4.8 million and receivables understatement of \$23.8 million.</p> <p>We recommend the Employment Security Department implement a process to correct the error in their certified uncollectible amounts.</p>
--	--



## State of Washington

### NOTES

We communicated this error to Meghan Phelps, Treasury Manager, Ibrahim Dembele, Treasury Director, Stephanie Eskesen, Audit Liaison, and Jay Summers, Audit Director on October 10, 2024.

See LOR: [\[LOR Summary\]](#).

### ISS.18 - V: OFM\_Allocation of OPEB Amounts (Part of ML)

<i>Prepared By:</i> BM2, 10/21/2024 <i>Reviewed By:</i> CJG, 1/8/2025 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<i>Issue</i> The Office of Financial Management (OFM) allocated Other Post employment Benefits (OPEB) balances across opinion units based on incorrectly calculated allocation percentages. As a result, the following balances were misstated:  Statement of Net Position (Government Wide) - Business-Type Activities: Long Term Liabilities Due in More Than One Year (Other Post Employment Benefits Obligations) was overstated by \$7.05 million Deferred Inflows of Resources (OPEB) was understated by \$8.63 million Statement of Net Position (Proprietary Funds) - Health Insurance: Other Long Term Liabilities - Noncurrent (Other Post Employment Benefits) was overstated by \$155 thousand. Statement of Net Position (Proprietary Funds) - Higher Education Student Services: Other Long Term Liabilities - Noncurrent (Other Post Employment Benefits) was overstated by \$8.75 million Deferred Outflows of Resources (OPEB) was overstated by \$946 thousand Deferred Inflows of Resources (OPEB) was understated by \$7.00 million  We recommend OFM perform a thorough review of underlying calculations related to OPEB balances to ensure they are accurately allocated across opinion units.
---	--

## State of Washington

### NOTES

We communicated this issue to Kennesy Cavanah, Statewide Accountant, on October 14, 2024.

See LOR here [[LOR Summary](#)].

See AOM here [[Aggregation of Misstatements \(GAAP\)](#)].

**INCLUDED IN ML at Iss. 40**

### ISS.20 - V: Bellevue College\_Confidential\_System User Access IT Controls

*Prepared By:* JLE, 10/17/2024  
*Reviewed By:* CJG, 11/1/2024  
*Type:* Verbal Recommendation  
*Category:* IT Controls - Confidential  
*Reporting Level(s):*

#### *Issue*

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record may be limited**

Bellevue College allowed ctcLink system user access to budget combo code screens for four unauthorized individuals.

We recommend Bellevue College periodically review its system user roles for accuracy.

*Impact*

*Cost Savings:*

*Questioned Costs:*

### NOTES

We communicated this issue to Jennifer McMillan (Fiscal Reporting Manager) on 10/17/2024.

See LOR at: [[LOR Summary](#)].

### ISS.21 - E: HCA\_ProviderOne Override IT Controls\_Confidential

*Prepared By:* DLE, 10/17/2024  
*Reviewed By:* CJG, 11/6/2024

#### *Issue*

The Health Care Authority has the following weaknesses related to the process of forcing edits through the override process in the ProviderOne system:

## State of Washington

<p><i>Type:</i> Financial Statements</p> <p><i>Category:</i> IT Controls - Confidential</p> <p><i>Reporting Level(s):</i> Exit Item</p>   <p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i> \$0.00</p>	<p>Separation of duties between changing edits to forcible and forcing claims through edits was not system enforced.</p> <p>The Health Care Authority did not have a monitoring process in place to ensure that all claims that were forced through the override process were authorized.</p> <p>We recommend the Health Care Authority:</p> <p>Consider enforcing separation of duties between changing edits to forcible and forcing claims through edits.</p> <p>Implement a formal monitoring process to ensure that all claims forced through the override process are authorized. This should include a system generated report that specifically identifies overridden edits.</p>
--	---

### NOTES

#### **Communication of the Audit Issue with the Client:**

We verbally communicated the issue to Kari Summerour, External Audit Liaison, Dineen Kilmer, ProviderOne Section Manager, Ed Hicks, IT System Admin, and Angie Skinner IT System Admin, in a Teams meeting on 10/11/2024.

### ISS.22 - E: ESD\_Cash Reconciliation Variances

<p><i>Prepared By:</i> DRR, 10/23/2024</p> <p><i>Reviewed By:</i> CJG, 11/6/2024</p> <p><i>Type:</i> Financial Statements</p> <p><i>Category:</i> Accounting/Financial Reporting</p> <p><i>Reporting Level(s):</i> Exit Item</p>   <p><i>Impact</i></p>	<p><i>Issue</i></p> <p>The Employment Security Department was unable to reconcile their bank accounts to the accounting records at fiscal year end June 30, 2024. Various reconciling items totaling \$4,795,580 should not have been included in their respective reconciliations. We determined, after removing these reconciling errors from the reconciliations, cash &amp; cash equivalents was understated by \$9,090,932.</p> <p>We recommend the Employment Security Department:</p> <p>Update their bank reconciliation process to ensure it captures only cash activity, such as outstanding checks and deposits in transit.</p> <p>Perform a thorough review of the bank reconciliations to ensure they are accurate.</p>
--	---

## State of Washington

<i>Cost Savings:</i> <i>Questioned Costs:</i>	
<b>NOTES</b>	
<p>We communicated this error to Meghan Phelps, Treasury Manager, Ibrahim Dembele, Treasury Director, Stephanie Eskesen, Audit Liaison, and Jay Summers, Audit Director on October 23, 2024.</p> <p>LOR: <a href="#">[LOR Summary]</a></p>	
<b>ISS.24 - V: OFM - Reporting Entity (Part of ML)</b>	
<i>Prepared By:</i> RKM, 12/2/2024 <i>Reviewed By:</i> SHW, 12/9/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>   <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<i>Issue</i> <p>The Office of Financial Management (OFM) defines the state of Washington for reporting purposes and determining which organizations are financially accountable to the state and which other organizations that do not meet the financial accountability criteria should be included in the reporting entity if the nature and significance of their relationship with the state are such that exclusion would cause the state's financial statements to be misleading. OFM incorrectly reported the following:</p> <ul style="list-style-type: none"> <li>Excluded two related organizations in the reporting entity note disclosure.</li> <li>Included one entity as part of the primary government that should have been disclosed as a joint venture with equity interest.</li> <li>Excluded six entities from being discretely presented component units.</li> <li>Excluded one blended component unit in the reporting entity note disclosure.</li> <li>Excluded all commodity commissions from being reported as part of the primary government.</li> </ul> <p>We estimate OFM made the following understatements:</p> <ul style="list-style-type: none"> <li>Assets/Deferred Outflows - \$32 million</li> <li>Liabilities/Deferred Inflows - \$19 million</li> <li>Revenues - \$8 million</li> <li>Expenses - \$7 million</li> </ul> <p>Also, OFM did not have a process in place to identify or track related party transactions that would also require disclosure. These reporting errors are not</p>

## State of Washington

		significant to the State's financial statements.  We recommend OFM thoroughly review the reporting entity note disclosure to ensure all information is accurate and develop a process to identify or track related party transactions. We also recommend OFM to continue to assess materiality for agencies that are excluded from reporting.
<b>NOTES</b>		
See LOR Summary here: <a href="#">[LOR Summary]</a>		
We communicated this issue to Stacie Boyd, Statewide Accountant, on December 2, 2024. <b>INCLUDED IN ML at Iss. 40</b>		
<b>ISS.25 - E: Seattle Colleges_Misstatement of Education Expenses (Payroll)</b>		
<i>Prepared By:</i> EZM, 10/29/2024 <i>Reviewed By:</i> CJG, 11/25/2024 <i>Type:</i> Financial Statements <i>Category:</i> Payroll/Personnel <i>Reporting Level(s):</i>  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00		<i>Issue</i> Seattle Colleges did not provide adequate supporting documentation for payroll payments totaling \$69,121 made to 7 of the 30 employees we selected for testing. Based on our sample tests we estimate total unsupported payroll payments for the year to be \$6,869,128.  We recommend that Seattle Colleges ensure adequate supporting documentation is maintained and available for audit for all payroll expenditures.
<b>NOTES</b>		
LOR Summary: <a href="#">[LOR Summary]</a>		
Communication: We communicated this issue to Petrina Sims, Payroll Manager, on October 28, 2024.		

## State of Washington

### ISS.27 - V: DOT\_RSI Modified Approach: Infrastructure - Pavement

<i>Prepared By:</i> NJH, 11/5/2024 <i>Reviewed By:</i> RKM, 11/13/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	<i>Issue</i> The Department of Transportation did not provide pavement assessment data for inclusion in the <i>Required Supplementary Information</i> of the State ACFR. GASB Codification 1400.106 requires governments to document that a complete condition assessment of eligible infrastructure assets is performed in a consistent manner at least every three years. The Department of Transportation's internal procedure is to perform this assessment every two years.  We recommend the Department of Transportation complete pavement assessments in alignment with their internal two-year cycle and be able to provide documentation to the auditor for inspection.
--	--

### NOTES

We communicated this issue to Jesse Daniels, Audit Liasion, on 11/6/24.

See LOR at [[LOR Summary](#)].

### ISS.28 - F: The State lacked adequate internal controls over financial reporting to ensure college scholarship allowances were accurately reported

<i>Prepared By:</i> SHW, 12/3/2024 <i>Reviewed By:</i> CJG, 1/8/2025 <i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting	<i>Issue</i> <b>2024-001      The State lacked adequate internal controls over financial reporting to ensure college scholarship allowances were</b>
---	---

## State of Washington

<p><i>Reporting Level(s):</i> Finding</p> <p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i> \$0.00</p>	<p><b>accurately reported</b></p> <p><b><i>Background</i></b></p> <p>Scholarship discounts and allowances are the difference between a college or university's stated charge for goods and services and the amount the students or third parties paid for those goods and services. Student tuition and fee revenues, and certain other revenues from students, should be reported net of scholarship discounts and allowances in the Statement of Revenues, Expenses and Changes in Net Position and the Statement of Activities. In fiscal year 2024, the Office of Financial Management (OFM) estimated state colleges and universities had \$552 million in scholarship discounts and allowances.</p> <p><b><i>Description of Condition</i></b></p> <p>OFM did not calculate and report college and university scholarship discounts and allowances in the state's financial statements.</p> <p><b><i>Cause of Condition</i></b></p> <p>OFM was unaware that colleges and universities were making off-book adjustments to reported scholarship allowances when preparing their own financial statements and assumed those adjustments were in the state's accounting system.</p> <p><b><i>Effect of Condition</i></b></p> <p>OFM used scholarship discounts and allowance data that</p>
---	--

## State of Washington

	<p>colleges reported in prior periods to estimate the amount for fiscal year 2024. By not correctly reporting scholarship discounts and allowances, OFM made the following estimated misstatements:</p> <p>Higher Education Special Revenue Fund - Charges for services were understated and education expenditures were understated by \$189 million.</p> <p>Higher Education Student Service Fund - Charges for services were overstated and miscellaneous expenses were overstated by \$35 million.</p> <p>Governmental Activities - Charges for services were overstated and higher education expenses were overstated by \$327 million.</p> <p>Business-Type Activities - Charges for services were overstated and higher education student services expenses were overstated by \$35 million.</p> <p>These errors were corrected in the financial statement.</p> <p><b><i>Recommendation</i></b></p> <p>We recommend OFM establish a process to obtain timely scholarship discount and allowance data for all state colleges and universities for inclusion in the state's financial statements.</p> <p><b><i>Agency's Response</i></b></p>
--	---



## State of Washington

### ***Auditor's Remarks***

### ***Applicable Laws and Regulations***

*Government Auditing Standards*, July 2018 Revision, paragraphs 6.40 and 6.41 establish reporting requirements related to significant deficiencies or material weaknesses in internal control, instances of fraud, and noncompliance with provisions of laws, regulations, contracts, or grant agreements.

The American Institute of Certified Public Accountants defines significant deficiencies and material weaknesses in its *Codification of Statements on Auditing Standards*, section 265, Communicating Internal Control Related Matters Identified in an Audit, paragraph 7.

RCW 43.88.160 Fiscal management – Powers and duties of officers and agencies, states in part:

(4) In addition, the director of financial management, as agent of the governor, shall:

(a) Develop and maintain a system of internal controls and internal audits comprising methods and procedures to be adopted by each agency that will safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies for accounting and financial controls. The system developed by the director shall include criteria for determining the scope and

## State of Washington

	<p>comprehensiveness of internal controls required by classes of agencies, depending on the level of resources at risk.</p> <p><i>GASB 34, Paragraph 100, Footnote 41</i>, pertaining to the operating statements for proprietary funds states: "Revenues should be reported net of discounts and allowances with the discount or allowance amount parenthetically disclosed on the face of the statement or in a note to the financial statements. Alternatively, revenues may be reported gross with the related discounts and allowances reported directly beneath the revenue amount".</p> <p><i>GASB Implementation Guide No. 2015-1 70.40.3</i> clarifies this requirement also applies to the statement of activities "Consistent with the requirements in Statement 33 and footnote 41 to paragraph 100 of Statement 34, exchange revenues for governmental activities should be reported net of uncollectible accounts".</p>
<b>NOTES</b>	

### ISS.29 - V: WSU\_Federal Revenue (Part of ML)

<i>Prepared By:</i>	EZM, 11/18/2024	<i>Issue</i>
<i>Reviewed By:</i>	CJG, 11/25/2024	Washington State University reported receipts of Federal Direct Student loans as federal revenue within ALN 84.268, rather than a reduction in expenditures. This resulted in an overstatement of Federal Grants in Aid revenue of \$145,140,687 and a corresponding overstatement in expenditures within the Special Revenue Funds - Higher Education.
<i>Type:</i>	Verbal Recommendation	
<i>Category:</i>	Accounting/Financial Reporting	
		We recommend the Office of Financial Management work with Washington State

## State of Washington

<i>Reporting Level(s):</i>	University in their reconciliation of Direct Federal Assistance to ensure the proper accounting and recording of federal revenues.
<i>Impact</i>	
<i>Cost Savings:</i>	
<i>Questioned Costs:</i>	

### NOTES

LOR Summary: [[LOR Summary](#)]

We communicated this issue to Marina Yee, OFM Statewide Accounting Supervisor, on November 15, 2024, and Kim Small, WSU Director of Sponsored Program Services, on November 18, 2024.

**INCLUDED IN ML at Iss.40**

### ISS.30 - E: DOT\_SEFA and TRAINS to AFRS Reconciliation

<i>Prepared By:</i>	EZM, 11/18/2024	<i>Issue</i>
<i>Reviewed By:</i>	CJG, 1/8/2025	The Department of Transportation is unable to fully reconcile federal grants in aid revenue reported within TRAINS and on the SEFA to rollup amounts within AFRS. This resulted in an overstatement of \$59,302,503 for Federal Grants in Aid in Aggregate Remaining Funds.
<i>Type:</i>	Financial Statements	
<i>Category:</i>	Accounting/Financial Reporting	
<i>Reporting Level(s):</i>	Exit Item	We recommend that the Department of Transportation work with Office of Financial Management in their reconciliation of Direct Federal Assistance to ensure that federal revenues are correctly reported in the financial statements.
<i>Impact</i>		
<i>Cost Savings:</i>		
<i>Questioned Costs:</i>		

### NOTES

## State of Washington

LOR Summary: [\[LOR Summary\]](#)

We communicated this issue to Marina Yee, OFM Statewide Accounting Supervisor, and Suzi Freelund, WSDOT Accounting and Reporting Manager, on November 15, 2024.

### ISS.31 - E: SBCTC\_Questionable Balances

<i>Prepared By:</i> DRR, 11/19/2024 <i>Reviewed By:</i> RKM, 12/17/2024 <i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Exit Item  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	<i>Issue</i> The state produces a series of year-end exception reports designed to identify potential errors in financial reporting. Based on our review of these reports, we found a number of likely errors that should have been investigated and corrected. The State Board for Community & Technical Colleges (SBCTC) did not actively work, investigate, and adjust a number of the high-risk balances noted in these reports including:  <u>Assets with credit balance</u> Fund 450 GL 1110 Cash in Bank (\$4,954,750). Fund 790 GL 1318 Unbilled Receivables (\$1,641,146). Fund 859 GL 1110 Cash in Bank (\$2,148,656).  <u>Liabilities with debit balance</u> Fund 145 GL 5181 Employee Insurance Deductions Payable \$1,922,085. Fund 846 GL 5190 Unearned Revenues \$1,596,204.  These potential errors were not corrected in the financial statements.  We recommend SBCTC actively investigate and adjust balances when appropriate.
---	--

### NOTES

We communicated this issue to Sue Willis, ctclink Accounting Coordinator, Anna Quichocho, Statewide Accountant on November 19, 2024.

See LOR [\[LOR Summary\]](#)

## State of Washington

See AOM [[Aggregation of Misstatements \(GAAP\)](#)]

### ISS.32 - V: OFM\_Financial Disclosures - Lack of follow up on missing disclosures

<i>Prepared By:</i> EZM, 11/19/2024 <i>Reviewed By:</i> CJG, 11/21/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Other <i>Reporting Level(s):</i>  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	<i>Issue</i> The University of Washington is required, per RCW 43.88.160(4)(a), to have an internal audit function, and to submit an internal audit certification annually to the Office of Financial Management as part of their Financial Disclosure certifications. The University did not submit an internal audit certification this year, and the Office of Financial Management did not follow up with the University on this missing disclosure.  We recommend the Office of Financial Management work with the University to ensure that they submit all of their required disclosures.
---	---

### NOTES

LOR Summary: [[LOR Summary](#)]

Communication: We communicated this issue to Kenney Cavanah, OFM Statewide Accountant, on November 19, 2024.

### ISS.33 - V: OFM\_WSHFC (Part of Finding 2024-002)

<i>Prepared By:</i> NJH, 11/20/2024 <i>Reviewed By:</i> RKM, 12/6/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting	<i>Issue</i> The Office of Financial Management (OFM) did not correctly recalculate the net investment in capital assets and did not report all audited amounts for the Washington State Housing & Finance Commission (WSHFC). As a result, the following balances were misstated:  <u>Nonmajor Component Units Combining Statement of Net Position</u> Cash and cash equivalents was understated by \$260 million Investments was understated by \$106 million
--	--

## State of Washington

<p><i>Reporting Level(s):</i></p>     <p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i></p>	<p>Receivables (net of allowance) was understated by \$2.2 million Prepaid expenses was understated by \$2.7 million Other noncurrent assets was understated by \$741.0 million Deferred outflows of resources was overstated by \$1.5 million Accounts payable was understated by \$293.7 million Accrued liabilities was overstated by \$39.5 million Other noncurrent liabilities was understated by \$740.4 million Deferred inflows of resources was understated by \$3.3 million Net investment in capital assets was overstated by \$763 thousand Restricted for other purposes was understated by \$112.3 million Unrestricted net position was understated by \$763 thousand</p> <p><u>Nonmajor Component Units Combining Statement of Revenues, Expenses, and Changes in Net Position</u></p> <p>Expenses understated by \$38.7 million Charges for services overstated by \$1.8 million Operating grants and contributions understated by \$25.4 million Earning (loss) on investments understated by \$23.0 million</p> <p>We recommend the OFM carefully follow the net investment in capital assets calculation described in GFOA 6-002-09 for all non-major component units. We also recommend OFM to report all amounts in component unit audited financial statements.</p>
<b>NOTES</b>	
<p>We communicated this issue to Stacie Boyd (OFM) on 11/20/24 and Anna Quichocho (OFM) on 12/4/2024.</p> <p>See LOR at [<a href="#">LOR Summary</a>].</p> <p><b>INCLUDED IN Finding 2024-002 at Iss. 43</b></p>	
<b>ISS.34 - V: OFM_Budget to GAAP Reconciliation (Part of ML)</b>	
<i>Prepared By:</i>	<i>Issue</i>

## State of Washington

<p><i>Reviewed By:</i> RKM, 12/10/2024</p> <p><i>Type:</i> Verbal Recommendation</p> <p><i>Category:</i> Accounting/Financial Reporting</p> <p><i>Reporting Level(s):</i></p>   <p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i> \$0.00</p>	<p>The Office of Financial Management reported misstatements on 16 lines of the Budgetary Comparison Schedule - Budget to GAAP Reconciliation for the Wildlife and Natural Resources Special Revenue Fund, as follows:</p> <p>Actual amounts (budgetary basis) "Total Resources" from the Budgetary Comparison Schedule - understated by \$2,901,320,000</p> <p>Transfers from other funds - understated by \$481,693,000</p> <p>Budgetary fund balance at the beginning of the biennium, as restated - understated by \$1,783,999,000</p> <p>Appropriated loan principal repayment - understated by \$61,477,000</p> <p>Noncash revenues - overstated by \$25,238,000</p> <p>Other revenues - overstated by \$189,244,000</p> <p>Biennium total revenues - understated by \$359,745,000</p> <p>Nonappropriated activity (revenues) - overstated by \$6,930,109,000</p> <p>Total Revenues (GAAP Basis) as reported on the Statement of Revenues, Expenditures, and Changes in Fund Balances - Governmental Funds - overstated by \$6,570,364,000</p> <p>Actual amounts (budgetary basis) "Total Charges to Appropriations" from the Budgetary Comparison Schedule - understated by \$166,293,000</p> <p>Appropriated transfers to other funds - overstated by \$167,358,000</p> <p>Other transfers to other funds - understated by \$687,235,000</p> <p>Appropriated loan disbursements - understated by \$269,876,000</p> <p>Biennium total expenditures - overstated by \$812,676,000</p> <p>Nonappropriated activity (expenditures) - overstated by \$6,926,361,000</p> <p>Total expenditures (GAAP basis) as reported on the Statement of Revenues, Expenditures, and Changes in Fund Balance - Governmental Funds - overstated by \$7,739,037,000</p> <p>We recommend the Office of Financial Management perform a thorough review of reconciliations and schedules to ensure they are accurately reported.</p>
<p><b>NOTES</b></p>	



## State of Washington

Level of Reporting Summary: [\[LOR Summary\]](#)

We verbally communicated this issue to Laura Lopez, Statewide Accountant, OFM, on Wednesday, November 20, 2024, via Teams. Laura confirmed that the issue will be corrected before final publication of the 2024 ACFR.

**INCLUDED IN ML at ISS. 40**

### ISS.35 - V: OFM\_GASB 100 - Accounting Changes (Part of ML)

<i>Prepared By:</i> BM2, 11/22/2024 <i>Reviewed By:</i> RKM, 12/6/2024 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>	<i>Issue</i> The Office of Financial Management (OFM) incorrectly classified accounting changes and error corrections on the Governmental Funds Statement of Revenues, Expenditures, and Changes in Fund Balances and Nonmajor Special Revenue Funds Combining Statement of Revenues, Expenditures, and Changes in Fund Balances by \$3.1 billion. OFM should have presented the changes and corrections as a single line on the statements or individually. Also, OFM did not properly disclose two error corrections in the notes to the financial statements as required by GASB 100.
<i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	We recommend the OFM report and disclose all accounting change and error corrections in accordance with GASB 100.

### NOTES

See LOR [\[LOR Summary\]](#)

We communicated this issue to Anna Quichocho, Financial Reporting Manager, on November 21, 2024, and November 22, 2024. OFM will not modify the disclosure in the final statements.

**INCLUDED IN ML at Iss. 40**

### ISS.35 - V: OFM\_GASB 100 - Accounting Changes (Part of ML)

<i>Prepared By:</i> BM2, 11/22/2024 <i>Reviewed By:</i> RKM, 12/6/2024	<i>Issue</i> The Office of Financial Management (OFM) incorrectly classified accounting changes and error corrections on the Governmental Funds Statement of
---	---



## State of Washington

<p><i>Type:</i> Verbal Recommendation</p> <p><i>Category:</i> Accounting/Financial Reporting</p> <p><i>Reporting Level(s):</i></p>	<p>Revenues, Expenditures, and Changes in Fund Balances and Nonmajor Special Revenue Funds Combining Statement of Revenues, Expenditures, and Changes in Fund Balances by \$3.1 billion. OFM should have presented the changes and corrections as a single line on the statements or individually. Also, OFM did not properly disclose two error corrections in the notes to the financial statements as required by GASB 100.</p>
<p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i> \$0.00</p>	<p>We recommend the OFM report and disclose all accounting change and error corrections in accordance with GASB 100.</p>

## NOTES

See LOR [[LOR Summary](#)]

We communicated this issue to Anna Quichocho, Financial Reporting Manager, on November 21, 2024, and November 22, 2024. OFM will not modify the disclosure in the final statements.

INCLUDED IN ML at Iss. 40

## ISS.38 - V: Exception Reports Analysis (Part of ML)

<p><i>Prepared By:</i> RKM, 11/27/2024</p> <p><i>Reviewed By:</i> SHW, 12/2/2024</p> <p><i>Type:</i> Verbal Recommendation</p> <p><i>Category:</i> Accounting/Financial Reporting</p> <p><i>Reporting Level(s):</i></p>	<p><i>Issue</i></p> <p>OFM runs a series of year-end exception reports designed to identify potential errors in financial reporting. We found OFM did not actively work and investigate several high-risk balances noted in these reports. Based on our review of the reports, we found several likely errors that should have been investigated and corrected, including:</p> <ul style="list-style-type: none"> <li>Due from other governments (\$60.8 million) should have been written off</li> <li>Claims and judgements payable (\$19.5 million) should have been liquidated</li> </ul>
<p><i>Impact</i></p> <p><i>Cost Savings:</i></p>	

## State of Washington

<i>Questioned Costs:</i>	Claims and judgements payable (\$8.2 million) requires further investigation  Assets (\$57.2 million) that likely needed adjustment  We recommend OFM actively investigate and adjust exception report balances when appropriate.
--------------------------	---

### NOTES

LOR: [\[LOR Summary\]](#)

We communicated this issue to Kennesy Cavanah, Statewide Accountant, on October 29, 2024.

**INCLUDED IN ML at ISS. 40**

### ISS.39 - V: OFM\_Subsequent Events - Bond Issuance

<i>Prepared By:</i> JLE, 11/25/2024 <i>Reviewed By:</i> CJG, 1/8/2025 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>     <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	<i>Issue</i> The Office of Financial Management incorrectly reported four bond issuances with a July 2024 issue date within Note 20 'Subsequent Events'. These bonds were issued in June 2024, and therefore should not have been disclosed as a subsequent event.  We recommend the Office of Financial Management enhance review procedures to ensure note disclosures are accurate.
--	---

### NOTES

We communicated this issue to Pam Valencia (OFM Statewide Accountant) and Anna Quichocho (Financial Reporting Manager) on 11/22/2024.

## State of Washington

ISS.40 - ML: OFM_Financial Statement Preparation	
<p><i>Prepared By:</i> RKM, 12/9/2024</p> <p><i>Reviewed By:</i> CJG, 12/9/2024</p> <p><i>Type:</i> Financial Statements</p> <p><i>Category:</i> Accounting/Financial Reporting</p> <p><i>Reporting Level(s):</i> Management Letter</p> <p><i>Impact</i></p> <p><i>Cost Savings:</i></p> <p><i>Questioned Costs:</i></p>	<p><i>Issue</i></p> <p><u>Management Letter</u> Office of Financial Management July 1, 2023 through June 30, 2024</p> <p><b>Financial Statement Preparation</b> The Office of Financial Management (OFM) is responsible for preparing the state's financial statements in accordance with generally accepted accounting principles (GAAP). These statements provide a thorough and detailed presentation of the state's overall financial condition. OFM is responsible for obtaining state agencies' financial data that is required to prepare these statements. At year-end, OFM is also responsible for ensuring the accuracy of the financial information presented in the statements.</p> <p>During the audit, we found instances in which the financial information presented in the financial statements were not accurate or was misclassified.</p> <p><i>Allocation of Other Postemployment Benefits (OPEB)</i></p> <p>OFM allocated OPEB balances across opinion units based on incorrectly calculated allocation percentages. As a result, the following balances were misstated:</p> <p>Statement of Net Position (Government Wide) - Business-Type Activities:</p> <p>Long-Term Liabilities Due in More Than One Year (OPEB) was overstated by \$7.1 million</p> <p>Deferred Inflows of Resources (OPEB) was understated by \$8.6 million</p> <p>Statement of Net Position (Proprietary Funds) - Health Insurance:</p> <p>Other Long-Term Liabilities - Noncurrent (OPEB) was overstated by \$155,000</p> <p>Statement of Net Position (Proprietary Funds) - Higher Education Student Services:</p> <p>Other Long-Term Liabilities - Noncurrent (OPEB) was overstated by \$8.8 million</p>

## State of Washington

	<p>Deferred Outflows of Resources (OPEB) was overstated by \$946,000 Deferred Inflows of Resources (OPEB) was understated by \$7 million</p> <p><i>Washington State University's Federal Assistance Reconciliation to AFRS Revenue</i> Washington State University reported receipts of Federal Direct Student Loans as federal revenue rather than a reduction in expenditures. This resulted in a \$145.1 million overstatement of Federal Grants in Aid revenue and a corresponding expenditures overstatement within the Higher Education Special Revenue Funds.</p> <p><i>Budgetary Comparison Schedule - Budget to GAAP Reconciliation</i> OFM incorrectly reported the entire Budgetary Comparison Schedule - Budget to GAAP Reconciliation for the Wildlife and Natural Resources Special Revenue Fund due to a formula error. The errors ranged from \$25.2 million to \$7.7 billion. This schedule is part of the Required Supplementary Information and the errors did not affect the reporting of the basic financial statements.</p> <p><i>GASB 100 Implementation</i> OFM incorrectly classified accounting changes and error corrections on the Governmental Funds Statement of Revenues, Expenditures, and Changes in Fund Balances and Nonmajor Special Revenue Funds Combining Statement of Revenues, Expenditures, and Changes in Fund Balances by \$3.1 billion. OFM should have presented the changes and corrections as a single line on the statements or individually. Also, OFM did not properly disclose two error corrections in the notes to the financial statements as required by GASB 100.</p> <p><i>Reporting Entity and Related Party Transactions</i> OFM defines the state of Washington for reporting purposes and determining which organizations are financially accountable to the state and which other organizations, that do not meet the financial accountability criteria, should be included in the reporting entity. OFM makes this determination by assessing if the nature and significance of the organization's relationship with the state are such that exclusion would cause the state's financial statements to be misleading. OFM incorrectly reported the following: Two related organizations were excluded in the reporting entity note disclosure</p>
--	---

## State of Washington

	<p>One entity was included as part of the primary government that should have been disclosed as a joint venture with equity interest</p> <p>Six entities were excluded from being discretely presented component units</p> <p>One blended component unit was excluded in the reporting entity note disclosure</p> <p>All commodity commissions were excluded from being reported as part of the primary government.</p> <p>Also, OFM did not have a process to identify or track related party transactions that would require disclosure. These reporting errors are not significant to the state's financial statements.</p> <p><i>Use of Exception Reports</i></p> <p>OFM runs a series of year-end exception reports designed to identify potential errors in financial reporting. We found OFM did not actively work and investigate several high-risk balances noted in these reports. Based on our review of the reports, we found several likely errors that should have been investigated and corrected, including:</p> <ul style="list-style-type: none"><li>Due from other governments (\$60.8 million) should have been written off</li><li>Claims and judgements payable (\$19.5 million) should have been liquidated</li><li>Claims and judgements payable (\$8.2 million) required further investigation</li><li>Assets (\$57.2 million) that likely needed adjustment</li></ul> <p><i>Investments Misclassification</i></p> <p>OFM is responsible for preparing a Statement of Net Position – Component Units based on the various component unit financial statements it obtains. OFM understated current investments for the Fred Hutchinson Cancer Center by \$646.2 million and overstated noncurrent investments by \$646.2 million.</p> <p>We recommend OFM:</p> <ul style="list-style-type: none"><li>Perform a thorough review of underlying calculations related to OPEB balances to ensure they are accurately allocated across opinion units</li><li>Assist Washington State University in its reconciliation of Direct Federal Assistance to ensure the proper accounting and recording of federal revenues</li></ul>
--	---

## State of Washington

	<p>Perform a thorough review of reconciliations and schedules to ensure they are accurately reported</p> <p>Thoroughly review the reporting entity note disclosure to ensure all information is accurate and develop a process to identify or track related party transactions</p> <p>Correctly report entities that are part of the state in accordance with GASB Statements 14 and 80</p> <p>Report and disclose all accounting change and error corrections in accordance with GASB 100.</p> <p>Actively work and investigate high-risk balances identified in its year-end exception reports</p> <p>Conduct a sufficient review to ensure financial statement balances are accurately reported</p> <p><u>Management Letter</u> Health Care Authority July 1, 2023 through June 30, 2024</p> <p><b><u>ProviderOne System</u></b> The Health Care Authority (HCA) contracts with a vendor for its Medicaid payment system, ProviderOne. During the fiscal year that ended June 30, 2024, ProviderOne processed about 141 million Medicaid transactions totaling \$18 billion. In the prior 11 audits, we recommended HCA obtain a Service Organization Control (SOC 2) report that covers an entire fiscal year.</p> <p>Although HCA's controls have improved, we found its SOC 2 report covered only six months of the fiscal year. This report is essential because it determines whether controls are properly designed and operating as intended in the processing and recording of Medicaid payments.</p> <p>Without a complete annual SOC 2 report, HCA risks inaccurate financial reporting in the state's general fund. HCA also risks having ineffective internal controls, which could lead to misuse, loss or misappropriation, inaccurate payments, and unauthorized software changes to the ProviderOne system.</p>
--	--

## State of Washington

	<p>Also, HCA receives and reviews the SOC 2 report to determine whether there are exceptions that require corrective action. However, HCA did not maintain documentation to support there was a SOC 2 report review. HCA has no documented procedures for receiving and reviewing the SOC 2 report to ensure it adequately and consistently performs the review.</p> <p>We recommend HCA continue to work with its vendor to obtain an annual SOC 2 report that covers the entire fiscal year. We also recommend HCA implement formal procedures for receiving and reviewing the report to include maintaining documentation evidencing the review occurred and the results.</p> <p><u>Management Letter</u> Washington State University July 1, 2023 through June 30, 2024</p> <p><b>Cash and Accrued Liabilities</b> Management is responsible for ensuring adjusting entries are input in the Agency Financial Reporting System (AFRS). Washington State University (WSU) did not include an adjusting entry in AFRS. This was due to there being a translation error between the University's chart of accounts and the AFRS chart of accounts. This caused the amount of cash and cash equivalents to be overstated and accrued liabilities to be overstated by \$267.8 million. This error was corrected in the state's financial statements.</p> <p>We recommend WSU perform a thorough review to ensure all entries are recorded in the state's accounting system.</p>
<b>NOTES</b>	
<p>LOR: <a href="#">LOR Summary</a></p> <p>This is a combined management letter of issues 4, 18, 24, 29, 34, 35, 38, 41 and 44. See communication in the respective issues.</p>	

## State of Washington

### ISS.41 - V: Component Units - Investments Misclassification (Part of ML)

<i>Prepared By:</i> NJH, 11/26/2024 <i>Reviewed By:</i> CJG, 1/8/2025 <i>Type:</i> Verbal Recommendation <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i>	<i>Issue</i> The Office of Financial Management (OFM) misclassified current & non-current investments for Fred Hutchinson Cancer Center on the component unit Statement of Net Position. Investments, current was understated by \$646.1M and the investments, noncurrent were overstated by \$646.1M.  We recommend OFM conduct a sufficient review to ensure line items are reported correctly.
<i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i> \$0.00	

### NOTES

We communicated this issue to Stacie Boyd (OFM) on 11/26/24.

See LOR at [[LOR Summary](#)].

**INCLUDED IN ML at ISS. 40**

### ISS.42 - E: WSU\_Bank Reconciliation Review Documentation

<i>Prepared By:</i> DRR, 11/26/2024 <i>Reviewed By:</i> CJG, 1/8/2025 <i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Exit Item	<i>Issue</i> Washington State University did not document their bank reconciliation review.  We recommend the University ensure that they are documenting who performed the reconciliation, who reviewed/approved the reconciliation and the date the review was performed.
--	--



## State of Washington

<i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	
<b>NOTES</b>	
We communicated the issue to Angie Dobbins, Executive Director/Controller, and Tami Bidle, Associate Controller, on November 26, 2024.	
See LOR: <a href="#">[LOR Summary]</a> .	

ISS.43 - F: Discretely Presented Component Units	
<i>Prepared By:</i> SHW, 12/6/2024 <i>Reviewed By:</i> CJG, 1/8/2025 <i>Type:</i> Financial Statements <i>Category:</i> Accounting/Financial Reporting <i>Reporting Level(s):</i> Finding  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	<i>Issue</i> <b>2024-002 The State lacked adequate internal controls over financial reporting to ensure it reported all discretely presented component unit financial activity in its financial statements.</b>  <b><i>Background</i></b>  State management is responsible for designing, implementing and maintaining internal controls that provide reasonable assurance financial statements are fairly presented and financial reporting is reliable. We identified deficiencies in internal controls that could adversely affect the State's ability to prevent, or quickly detect and correct, misstatements in the financial statements.  Washington state universities and colleges obtain support from nonprofit foundations. These foundations generally

## State of Washington

	<p>raise, administer and invest funds and make expenditures to or for the benefit of the university or college. Although the foundations are separate legal entities, accounting standards require the State to report their financial activity as discretely presented component units in the state's financial statements.</p> <p>The Washington State Housing Finance Commission (WSHFC) is a component unit of the state of Washington. It is a self-sustaining public agency committed to increasing housing access and affordability for Washington residents.</p> <p><i>Government Auditing Standards</i>, prescribed by the Comptroller General of the United States, requires the auditor to communicate material weaknesses in internal controls, as defined below in the Applicable Laws and Regulations section, as a finding.</p> <p><b><i>Description of Condition</i></b></p> <p>The Office of Financial Management (OFM) did not report the financial activity of the state university and college foundations as a component unit in the state's financial statements. Additionally, OFM did not report complete financial activity of the WSHFC in the state's financial statements.</p> <p>We consider this internal control deficiency to be a material weakness.</p> <p><b><i>Cause of Condition</i></b></p> <p>OFM deemed the financial activity of the foundations as</p>
--	--

## State of Washington

insignificant to the state's financial statements and elected not to report them. OFM staff also believed reporting complete financial information of the WSHFC was not appropriate as the state was not obligated for the entity's special assessment debt.

### ***Effect of Condition***

By not reporting university and college foundation financial activity and complete activity of the WSHFC, the state's component unit statement of net position and statement of revenues, expenses and changes in net position were materially misstated.

Although university and college foundation financial data for the fiscal year ending June 30, 2024, was not available at the time of our report, we estimated the following understatements based on prior years activity:

Assets/Deferred Outflows - \$1.5 billion

Liabilities/Deferred Inflows - \$65 million

Revenues - \$460 million

Expenses - \$379 million

OFM's omissions of certain WSHFC activity resulted in the following misstatements:

Assets and deferred outflows were understated by \$1.1 billion

Liabilities and deferred inflows were understated by \$998 million

## State of Washington

	<p>Net investment in capital assets were overstated by \$763,000</p> <p>Restricted for other purposes were understated by \$112.3 million</p> <p>Unrestricted net position were understated by \$763,000</p> <p>Expenses were understated by \$38.7 million</p> <p>Revenues were understated by \$46.6 million</p> <p>OFM did not correct these errors in the financial statements.</p> <p><b><i>Recommendation</i></b></p> <p>We recommend OFM establish a process to obtain timely financial information from university and college foundations to include in the state's financial statements. We further recommend OFM report complete financial information of the WSHFC as presented in its audited financial statements.</p> <p><b><i>Agency's Response</i></b></p> <p><b><i>Auditor's Remarks</i></b></p> <p><b><i>Applicable Laws and Regulations</i></b></p> <p><i>Government Auditing Standards, July 2018 Revision,</i></p>
--	--

## State of Washington

	<p>paragraphs 6.40 and 6.41 establish reporting requirements related to significant deficiencies or material weaknesses in internal control, instances of fraud, and noncompliance with provisions of laws, regulations, contracts, or grant agreements.</p> <p>The American Institute of Certified Public Accountants defines significant deficiencies and material weaknesses in its <i>Codification of Statements on Auditing Standards</i>, section 265, Communicating Internal Control Related Matters Identified in an Audit, paragraph 7.</p> <p>RCW 43.88.160 Fiscal management – Powers and duties of officers and agencies, states in part:</p> <p>(4) In addition, the director of financial management, as agent of the governor, shall:</p> <p>(a) Develop and maintain a system of internal controls and internal audits comprising methods and procedures to be adopted by each agency that will safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies for accounting and financial controls. The system developed by the director shall include criteria for determining the scope and comprehensiveness of internal controls required by classes of agencies, depending on the level of resources at risk.</p> <p><i>GASB 39 (codified at 2100.141)</i> requires reporting as a discretely presented component unit of legally separate, tax-exempt entities that meet all the following criteria:</p> <ol style="list-style-type: none"><li>1. Economic resources received or held by the separate organization are entirely or almost</li></ol>
--	---

## State of Washington

		<p>entirely for the direct benefit of the primary government, its component units, or its constituents.</p> <p>2. The primary government, or its component units, is entitled to, or has the ability to otherwise access, a majority of the economic resources received or held by the separate organization.</p> <p>3. Economic resources received or held by an individual organization that the specific primary government, or its component units, is entitled to, or has the ability to otherwise access, are significant to that primary government.</p>
<b>NOTES</b>		
LOR: <a href="#">[LOR Summary]</a> .		
We communicated this issue to Anna Quichocho and Sara Rupe of OFM on 11/26/2024 and 12/4/2024.		
<b>ISS.44 - V: WSU_Cash and Accrued Liabilities (Part of ML)</b>		
<i>Prepared By:</i>	RKM, 12/6/2024	<i>Issue</i> Management is responsible for ensuring adjusting entries are input in the Agency Financial Reporting System (AFRS). The Washington State University (WSU) did not include an adjusting entry in the AFRS. This was due to there being a translation error between the University's chart of accounts and AFRS chart of accounts. This caused the amount of cash and cash equivalents to be overstated and accrued liabilities to be overstated by \$267.8 million. This error was corrected in the state's financial statements.
<i>Reviewed By:</i>	CJG, 12/9/2024	
<i>Type:</i>	Verbal Recommendation	
<i>Category:</i>	Accounting/Financial Reporting	
		We recommend WSU perform a thorough review to ensure all entries are recorded

## State of Washington

<i>Reporting Level(s):</i>  <i>Impact</i> <i>Cost Savings:</i> <i>Questioned Costs:</i>	in the State's accounting system.
<b>NOTES</b>	
See LOR at: <a href="#">[LOR Summary]</a> .  We communicated this issue to Anna Quichocho, Financial Reporting Manager, and Angie Dobbins, Executive Director/Controller, on November 27, 2024. <b>INCLUDED IN ML at ISS. 40</b>	

### D.7.PRG - Due From Other Governments

*Procedure Step:* Controls - Year-end Accrual and Liquidations (HCA)  
*Prepared By:* EZM, 10/23/2024  
*Reviewed By:* SHW, 10/28/2024

Purpose/Conclusion.\*

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

# State of Washington

Testing Strategy:

**The following procedures are required for all significant systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.



## State of Washington

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Significant Balance(s) and Assertions**

Internal controls in the Receivable Accrual and Subsequent Liquidations address the following balance(s):

- **Due from Other Governments** - Amounts due from the Federal Government to reimburse program expenditures made by the state.

For the following assertions:

- **Existence** - Amounts due from the Federal Government to reimburse program expenditures are supported by amounts actually paid during the period and the underlying program expenditures.
- **Valuation** - Amounts due from the Federal Government to reimburse program expenditures have been calculated correctly.

## **Gain an Understanding of Internal Controls**

On October 21, 2024, we inquired with Kari Summerour, External Audit and Compliance Manager, regarding the internal controls for HCA's portion of the Due from Other Governments balance. She confirmed the understanding with the following individuals to ensure it was accurate for fiscal year 2024:

- Cheri Wright, Medicaid Accounting Manager
- Victoria Xu, Fiscal Analyst 4
- Laura Roberts, Federal Claims Supervisor
- Jill Arlow, Deputy Section Manager, Federal Financial Reporting

## *General Information*

All federal expenditures are recorded to cost objectives specific to the federal funding source. When a federal cost objective is established in AFRS, a corresponding federal revenue source is established and associated with the cost objective. Enterprise Reporting uses this structure to

## State of Washington

produce a report specifically developed to compare the level of federal expenditures for a period to the federal revenue source associated with those expenditures, and calculates the amount to be accrued. This process ensures federal expenditures for the period match the level of federal revenue posted for the same period. The variance column represents total expenditures less total revenues and would be the amount of additional accrued revenue that would be required to be posted to adjust GL1351. An analysis is then performed by the Fiscal Analyst to ensure that the revenue accrual is accurately calculated and based on final expenditures that are recorded and submitted for reimbursement.

### **Monthly Accruals**

The accrual process is performed monthly through a series of JVs that are processed for the regularly scheduled draws. The monthly revenue accruals are booked with XX batches. The process for calculating the monthly receivable begins by running a "Revenue Accrual Calculation" report by Program/Fund/MajorSource/SubSource. The program query criteria will depend on the program for which the accrual is being done, e.g. program 200 would be Medicaid, and the remaining criteria would include General Fund 001, and Major Group 03 (federal revenue). The report details federal disbursements, federal accruals, total expenditures, cash receipts, revenue accruals, total revenue and variance by major source (federal agency) and sub source (cost objective).

These JVs are MAJVs and are automatically reversed the next fiscal month under XY batches and primarily serve for information and reporting purposes; since the the monthly accruals are automatically reversed, they do not impact the final line amount at the end of the year.

### **Year End (Hard Accrual)**

At year-end, the revenue is accrued using a regular JV batch. This establishes an actual accrual for the fiscal year close. This accrual will be liquidated in the following year as prior period revenue is received.

The first year-end JV is completed using a main JV number as a JV batch to differentiate from the other XH batches. All subsequent JV's will use the same main JV number with a suffix from the beginning of the alphabets to tie all the year-end JVs together. The JV process is the same as for all subsequent accruals in which a template is set up and the final expenditure and revenue reports are run to determine the final accrual to be posted (**Key Control #1 - Existence/Valuation - Year-end accrual amount is based upon final expenditure and revenue reports**). This accrual process occurs repeatedly during FMs 12-99 and 24-25 in order to obtain the most accurate and current expenditure/revenue amounts for the accrual calculation. A fiscal analyst analyzes the final year-end expenditures, revenue, and revenue draws to calculate the final revenue accrual to record the Due from Federal Governments amount.

### **How Transactions are Recorded in AFRS (YE Accrual):**

Transactions are recorded in AFRS using the JV process that is performed by the Fiscal Analyst during the calculation of the revenue accrual noted above. The workbook will provide the coding details for the transaction that will be needed to record the transaction in AFRS. The Fiscal Analyst will log into AFRS and check the JV batch for errors. If there are no errors, the batch is then released in AFRS and a screen print of the AFRS release screen is saved to the "Upload and Release" tab of the JV workbook. If there are errors, the Fiscal Analyst will then research the JV to identify the error before making a correction and resubmitting it to the Assistant Accounting Manager for re-approval; this process occurs for

## State of Washington

every accrual run during the close (**Key Control #2 - Year-end accrual reviews and approvals**)

### **Adjustments to the GL1351 Amount (prior periods)**

The "hard coded" revenue accruals from the prior period are adjusted as the expenditures and revenues are liquidated throughout the subsequent fiscal year; these expenditure/revenue liquidations are identified through MOS and Fiscal Year fields in the determination of current vs prior period transactions. This occurs during standard federal draw downs and the recording process as summarized in the Federal Grants in Aid understanding [Controls - HCA]. The revenue adjustment associated with liquidations are recorded with TC 835 to adjust the GL1351 recorded amount (**Key Control #3 - Valuation - Adjustments to prior period year-end accruals are based upon expenditure and revenue liquidations in the current period**).

### Key Controls:

- **Key Control #1 - Valuation/Existence - The year-end hard revenue accrual/receivable recording is prepared and calculated using year-end expenditure and revenue amounts for programs.**
- **Key Control #2 - Valuation/Existence - The year-end revenue accrual/receivable recording is reviewed at each subsequent rerun by the Accounting Manager to ensure the correct amounts are posted and for the correct revenue subsources.**
- **Key Control #3 - Valuation - During the Federal Grants in Aid draw down process, adjustments to the prior period's revenue accrual are based upon expenditure and revenue liquidations.**

### **Noted Weaknesses are as follows:**

- None.

### **D.7.PRG - Due From Other Governments**

*Procedure Step:* Key Control #1 and 2 (Manual) - Calculation and Review of YE Accrual

*Prepared By:* EZM, 10/28/2024

*Reviewed By:* SHW, 10/28/2024

Purpose/Conclusion:
---------------------

### **Purpose:**

To confirm the calculation, recording, and review of the year-end federal revenues accrual (key control #1 and #2 for the Year-End Accrual) in

## State of Washington

order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision,*

## State of Washington

*the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially*

## State of Washington

*be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Due From Other Governments - Valuation and Existence**

**Key Control #1** - The year-end hard revenue accrual/receivable recording is prepared and calculated using year-end expenditure and revenue amounts for programs.

**Key Control #2** - The year-end revenue accrual/receivable recording is reviewed at each subsequent rerun by the Assistant Accounting Manager to ensure the correct amounts are posted and for the correct revenue subsources.

The understanding for this system is documented above in the "Controls - Year-End Accrual and Liquidations (HCA)" step.

### **STEP 1: Confirm Key Controls**

We reviewed the series of year-end JVs for the federal revenue accrual process to determine whether the federal revenue accruals (receivable side):

- Existed at year end, i.e. were based upon actual program receipts and liquidations of expenditures and revenues, and
- were reported at correct values, i.e. correctly calculated based upon the program expenditures and revenues. The details of testing is documented at [\[Substantive Test\]](#).

We reviewed [\[HCA YE Accrual\]](#) the following JV documents:

- MAJV8189, 7/17/24
- MAJV8189-AA, 7/30/24
- MAJV8189-BB, 8/15/24
- MAJV8189-CC, 8/28/24
- MAJV8189-DD, 8/29/24
- MAJV8189-EE, 9/4/24

## State of Washington

and their supporting documentation, including Enterprise Reporting revenue/expenditures reports (**KC1**) and additional correspondence related to the JVs and recalculated the revenue accruals and compared them to recorded accruals (and corresponding receivable) with **no issues noted**. The criteria for each run of the ER reports were adequate to capture all federal revenues and expenditures for the agency and time frames. **No issues noted**.

We documented the preparer/submitter (Victoria Xu, FA4) and approver/releaser (Cheri Gullekson, Medicaid Accounting Manager) of the JVs and noted that there was evidence of review of the revenue subsources and calculations based upon the JV tabs. The preparer/submitter and approver/releasers were separate individuals (**KC2**). **No issues noted**.

### **STEP 2: Preliminary Control Risk Assessment**

**MAX** - We noted **no matters** involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 3: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.7.PRG - Due From Other Governments**

*Procedure Step:* Key Control #3 (Manual) - Accrual/Receivable Liquidations

*Prepared By:* EZM, 10/23/2024

*Reviewed By:* SHW, 10/28/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To confirm the calculation and recordings of receivable liquidations (key control #3 for Year-End Accrual and Liquidations) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.



# State of Washington

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important*

## State of Washington

*enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria.7

### **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:
----------------------

**Key Control #3 (Valuation): During the Federal Grants in Aid draw down process, adjustments to the prior period's revenue accrual are based upon expenditure and revenue liquidations.**

The understanding for this system is documented above in the "Controls - Year-End Accrual and Liquidations (HCA)" step.

## **STEP 1: Confirm Key Controls**

We reviewed current document FA0073 for the T19 Assistance 2024 weekly draw down revenue recording for the week of 2/05/24. The draw reconciliation was performed by Rossner Gideon, FA5. Included in the workbook were the two enterprise reporting reports used to calculate the draw amount. Relevant report criteria included:

- Expenditure report
  - Begin fiscal month - 01-Jul FY1
  - End fiscal month: Nov FY1
  - Cost objective: T4\*,D4\*,N4\*,Q4\*, [T44C\*,D44C\*,N44C\*,Q44C\*]
  - Cost allocation type: F
  - Expenditure content: Cash
  - Expenditure liquidation Content: All liquidations
- Revenue report
  - Begin fiscal month - 01-Jul FY1
  - End fiscal month: Nov FY1
  - Major source: 03
  - Source: 03/93
  - Subsource: 03/93/D4\*,03/93/T4\*,03/93/N4\*,03/93/Q4\*, [03/93/D44C\*,03/93/T44C\*,03/93/N44C\*,03/93/Q44C\*]
  - Revenue content: Cash
  - Revenue liquidation content: Yes

Cost objectives (Expenditures), as summarized:

- T\*\*\*:

## State of Washington

- Disbursements: 1,860,174,892.94
  - Liquidations: (136,817,662.55)
- D\*\*\*:
  - Disbursements: 907,638,005.39
  - Liquidations: (45,562,574.13)
- N\*\*\*: No activity
- Q\*\*\*: No activity

Revenue sub-sources (Revenues), as summarized:

- T\*\*\*:
  - Cash Receipts: 1,712,858,629.38
  - Liquidations: (137,626,213.55)
- D\*\*\*:
  - Cash Receipts: 907,851,661.12
  - Liquidations: (45,006,818.63)
- N\*\*\*: No activity
- Q\*\*\*: No activity

Totals:

Current Disbursements: 2,767,812,898.33

Current Receipts: 2,620,710,290.50

**Liquidations (Net):** 252,795.50

Draw Amount: 147,355,403.33

This total draw of \$147,355,403.33 appeared as the HCA portion of the total draw (draws include amounts from DSHS and DCYF as the Medicaid grant is administered through HCA) for PMS Subaccount XIX-MAP24. The reports were submitted by Rossner Gideon, FA5, to Laura Roberts, Federal Claims Supervisor, for review on 2/05/24, at 9:00 am, and the draw was approved by Laura Roberts at 9:15 on the same day.

As the liquidations were related to the prior period, the revenue recording workbook used TC835 for the net expenditure and revenue liquidations for the relevant subsource to adjust the accrual in GL1351. This was verified in the A8-A report with the:

- D\* transactions totaling \$(769,411.23) (as calculated by the revenue/expenditure report)
- T\* transactions totaling \$148,124,814.56 (as calculated by the revenue/expenditure report).

Total liquidation of the receivable: \$147,355,403.33

**No issues noted.**

# State of Washington

## **STEP 2: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **STEP 3: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.7.PR.G - Due From Other Governments**

*Procedure Step:* Controls - Year-end Accrual and Liquidations (DSHS)

*Prepared By:* EZM, 11/7/2024

*Reviewed By:* RKM, 11/8/2024

Purpose/Conclusion:

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

#### **The following procedures are required for all significant systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.

## State of Washington

- Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
- Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
- Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

## State of Washington

- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

# State of Washington

Record of Work Done:

## **Significant Balance(s) and Assertions**

Internal controls in the Receivable Accrual and Subsequent Liquidations address the following balance(s):

- **Due from Other Governments** - Amounts due from the Federal Government to reimburse program expenditures made by the state.

For the following assertions:

- **Existence** - Amounts due from the Federal Government to reimburse program expenditures are supported by amounts actually paid during the period and the underlying program expenditures.
- **Valuation** - Amounts due from the Federal Government to reimburse program expenditures have been calculated correctly.

## **Gain an Understanding of Internal Controls**

We inquired with Rick Meyer, External Audit Compliance Manager, on October 30, 2024 regarding the controls for DSHS's portion of the Due from Other Governments balance. He confirmed the prior year understanding with the following individuals to ensure it was accurate for fiscal year 2024:

- Christine Johnson, Administrative Services Manager
- Christina Choate, Program Services Manager
- Debra Trickler, ESA
- Julia Mosier, Office Chief (DDA/AL TSA)
- Rick Meyer, External Audit Liaison

The Office of Accounting Services (OAS) prepares revenue accruals monthly and at fiscal year-end. For both instances, the formula for determining the revenue accrual is:

Cash expenditures + Accrued Expenditures - Cash Revenue - Existing Accrued Revenue = Revenue to be accrued.

## **Monthly Revenue Accrual**

At fiscal month close, the Fiscal Analyst preparing the monthly accrual will run an Enterprise Reporting report "Revenue Accrual Calculation by Program/Account/Major Source/Source/Subsource". Relevant criteria includes:

- Agency: 300
- Fiscal Month: 1-11 or 13-23
- Account: 001
- Program: [080,850]
- Major Source: 03
- Source: 03/\*
- Subsource: [03/16/523\*\*,03/93/T19TR0,03/93/596\*\*\*,03/21/019V\*\*,03/93/498\*\*,03/99/APPTRN, 03/55/CMPRE0]



## State of Washington

The above subsources are excluded for varying reasons including: own funding, expenditures not tied to specific grant, etc.

This reports captures year-to-date expenditures, revenues, and liquidations for the relevant grant programs for the agency and is the basis for the monthly accrual calculations.

OAS has a monthly accrual JV log for preparers to fill information such as the JV number, date, and prepared by. The monthly accruals are prepared using XS batches, which automatically reverse using an XY batch upon subsequent monthly accruals, i.e. the monthly accruals do not impact the final Due from Other Governments line item.

The Fiscal Analyst will load the Enterprise Reporting report into the accrual workbook with minor formatting to create the toolbox for AFRS upload; the transactions use TC 051 (dr 1351, cr 3205) by subsource code for the accrual. The log is then updated with the JV hash amounts and submitted, the Program/Administrative Manager will review the batch for accuracy/calculations and approve it for release.

### **Year-End Accrual**

The year-end hard accrual is prepared in a similar manner as the monthly accruals in that the calculation is still the same:  
 $\text{Cash expenditures} + \text{Accrued Expenditures} - \text{Cash Revenue} - \text{Existing Accrued Revenue} = \text{Revenue to be accrued.}$

The year-end accrual is processed for fiscal months 12-99 and 24-25 and uses KH Batch types for recording. The procedures are performed at the below intervals:

- FM12 & FM24 - On the last working day of fiscal month
- FM99 & FM25 - On the last working day of Phase 1 for fiscal month
- FM99 & FM25 - Weekly; each Friday between Phase 1 (P1) close and Phase 1B (P1B) cutoff
- FM99 & FM25 – Daily; between Phase 1B (P1B) through Phase 2 (P2) close

The fiscal analyst will run the following report:

- Agency: 300
- Fiscal Month: 12 (or 12A, 24, 24A)
- Account: 001
- Program: [080,850]
- Major Source: 03
- Source: 03/\*
- Subsource: [03/16/523\*\*,03/93/T19TR0,03/93/596\*\*\*,03/21/019V\*\*,03/93/498\*\*,03/99/APPTRN, 03/55/CMPRE0]

The above subsources are excluded for varying reasons including: own funding, expenditures not tied to specific grant, etc.

## State of Washington

This reports captures year-to-date expenditures, revenues, and liquidations for the relevant grant programs for the agency and is the basis for the accrual calculation. **(Key Control #1 - Year-end accrual calculations - Valuation/Existence)**

Each subsequent run of the year-end accrual JV calculation to adjust (FM99/25) the original FM12/24 accrual will append a batch suffix AA, BB, CC, and so on to the JV.

The Fiscal Analyst will load the Enterprise Reporting report into the accrual workbook with minor formatting to create the toolbox for AFRS upload; the transactions (TC051) are by subsource code for each program, and the year-end log is then updated with the JV hash amounts and submitted. The Program/Administrative Manager will review the each of the accrual batches for verification of revenue subsources and calculation amounts and approve it for release.

### **How Transactions are Recorded in AFRS (YE Accrual):**

Transactions are recorded in AFRS using the JV process that is performed by the Fiscal Analyst during the calculation of the revenue accrual note above. The workbook will provide the coding details for the transaction that will be needed to record the transaction in AFRS. The Fiscal Analyst will log into AFRS and check the batch for errors. If there are no errors, the batch is then released in AFRS and a screen print of the AFRS release screen is saved to the "Upload and Release" tab of the JV workbook. If there are errors, the Fiscal Analyst will then research the JV to identify the error before making a correction and resubmitting it to the Program/Administrative Manager for re-approval. **(Key Control #2 - Year-end accrual review and approval - Valuation/Existence)**

### **Adjustments to the GL1351 Amount (prior periods)**

The "hard coded" revenue accruals from the prior period are adjusted as the expenditures and revenues are liquidated throughout the subsequent fiscal year; these expenditure/revenue liquidations are identified through MOS and Fiscal Year fields in the determination of current vs prior period transactions. This occurs during standard federal draw downs and their recording process as summarized in the Federal Grants in Aid understanding [[Controls - DSHS](#)]. The revenue adjustment associated with liquidations are recorded with TC835 or TC835(R) to adjust the GL1351 recorded amount. **(Key Control #3 - Prior period year-end accrual adjustments - Valuation)**

### **Key Controls are as Follows:**

- **Key Control #1 - Valuation/Existence - The year-end hard revenue accrual/receivable recording is prepared and calculated using year-end expenditure and revenue amounts for programs.**
- **Key Control #2 - Valuation/Existence - The year-end revenue accrual/receivable recording is reviewed at each subsequent rerun by the Administrative/Program Manager to ensure the correct amounts are posted and for the correct revenue subsources.**
- **Key Control #3 - Valuation - During the Federal Grants in Aid draw down process, adjustments to the prior period's revenue accrual are based upon expenditure and revenue liquidations.**

# State of Washington

## Noted Weaknesses are as Follows:

None

### D.7.PRG - Due From Other Governments

*Procedure Step:* Key Control #1 and 2 (Manual) - Calculation and Review of YE Accrual

*Prepared By:* EZM, 11/13/2024

*Reviewed By:* SHW, 11/14/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm the calculation, recording, and review of the year-end federal revenues accrual (key control #1 and #2 for the Year-End Accrual) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation.*

## State of Washington

*Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

## State of Washington

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Due From Other Governments - Valuation and Existence**

**Key Control #1** - The year-end hard revenue accrual/receivable recording is prepared and calculated using year-end expenditure and revenue amounts for programs.

**Key Control #2** - The year-end revenue accrual/receivable recording is reviewed at each subsequent rerun by the Administrative/Program Manager to ensure the correct amounts are posted and for the correct revenue subsources.

The understanding for this system is documented above in the "Controls - Year-End Accrual and Liquidations (DSHS)" step.

# State of Washington

## **1. Confirmation of Key Manual Control:**

We reviewed the series of year-end JVs for the federal revenue accrual process to determine whether the federal revenue accruals (receivable side):

- Existed at year end, i.e. were based upon actual program receipts and liquidations of expenditures and revenues, and
- were reported at correct values, i.e. correctly calculated based upon the program expenditures and revenues. The details of testing is documented at [Substantive Test].

DSHS processed a total of 14 year-end JVs (JVKH0015, base through suffix MM) from 7/15/2024 through 8/23/2024 to post their year-end receivable. We reviewed each run of the year-end accrual [DSHS YE Accrual] and their supporting documentation include Enterprise Reporting revenue/expenditure reports **(KC1)** and additional correspondence and recalculated the revenue accruals and compared them to recorded accruals with no issues noted. The criteria for the ER reports were adequate to capture all federal revenues and expenditures for the agency and time frames. **No issues noted.**

We documented the preparer/submitter/releaser (Sumanpreet Kaur, FA3 and Eddie Yang, FA4) and approver (Raiatea Arcuri, Senior Financial Coordinator, and Christina Choate, Program Services Manager) of the JVs and noted that there was evidence of review of the revenue subsources and calculations based upon the JV tabs. The preparer/submitter/releaser and approver were separate individuals **(KC2)**. **No issues noted.**

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **D.7.PRG - Due From Other Governments**

*Procedure Step:* Key Control #3 (Manual) - Accrual/Receivable Liquidations

*Prepared By:* EZM, 11/7/2024

# State of Washington

Reviewed By: SHW, 11/8/2024

Purpose/Conclusion:

**Purpose:**

To confirm the calculation and recordings of receivable liquidations (key control #3 for Year-End Accrual and Liquidations) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated"*

## State of Washington

*step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider



## State of Washington

*whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Due From Other Governments - Valuation and Existence**

**Key Control #3 - Valuation - During the Federal Grants in Aid draw down process, adjustments to the prior period's revenue accrual are based upon expenditure and revenue liquidations.**

The understanding for this system is documented above in the "Controls - Year-End Accrual and Liquidations (DSHS)" step.

### **1. Confirmation of Key Manual Control:**

We reviewed current document FA0047 (batch KX 139) for the T19 Assist weekly draw down revenue recording for the week of November 20, 2023. Included in the draw workbook was the draw report, prepared by Beverley Muncaster, Senior Financial Coordinator, sent to HCA for DSHS's portion of the weekly draw which contained (in summary, based upon draw calculations (Current) Expenditures - (Current) Revenues - Net Liquidations) for AFRS transaction dates 11/06/23 - 11/13/23:

D4\*

Net current = \$76,298,676.82

**Net liquidations = \$(1,582,080.32)**

Net draw = \$74,716,596.50

## State of Washington

T4\*

Net current = \$3,437,130.21

**Net liquidations = \$(188,629.81)**

Net draw = \$3,248,500.40

N4\*

Net current = \$0

**Net liquidations = \$(1,724.50)**

Net draw = \$(1,724.50)

As the liquidations were related to the prior period, the revenue recording workbook (Batch KX 443) used TC835 for the net expenditure and revenue liquidations for the relevant subresource to adjust the accrual in GL1351. The total amount for TC835 matched the draw calculations for the relevant cost objectives/subsource. This was verified in the "KX443" tab (AFRS upload transactions) with following as calculated by the revenue/expenditure reports and the GMS draw calculations:

D4\* transactions totaling **\$(1,582,080.32)**

T4\* transactions totaling **\$(188,629.81)**

N4\* transactions totaling **\$(1,724.50)**

The revenue recording workbook was prepared/submitted by Summaiya Khan, Fiscal Analyst 4, and approved by Gwendolyn Dain, Program Services Manager.

**No issues noted.**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **D.7.PRG - Due From Other Governments**

*Procedure Step:* Risk Assessment

# State of Washington

*Prepared By:* EZM, 11/7/2024

*Reviewed By:* RKM, 11/8/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*
  - *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

## State of Washington

- Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?
- Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.
- **Inherent Risk due to Fraudulent Reporting (intentional misstatements)**
  - Are there substantial pressures or motivations to misstate the balance?
- **Inherent Risk due to Misappropriation**
  - Is the account balance or transaction class susceptible to sizable misappropriation?
- **Inherent Risk due to Non-Compliance**
  - Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?
  - Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?
  - Are there any motivations or pressures to not comply?

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

## State of Washington

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- Year-End Accruals – Existence and Valuation: **MODERATE**
- Accrual/Receivable Liquidations - Valuation: **MODERATE**

# State of Washington

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

- **Year-End Accruals** – Existence and Valuation
- **Accrual/Receivable Liquidations** - Valuation

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

- Year-End Accruals – Existence and Valuation: **MODERATE**
- Accrual/Receivable Liquidations - Valuation: **MODERATE**

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

- Adjustments to Receivable balances - We plan to sample draw-down workbooks from HCA and DSHS, and review backup documentation including enterprise reporting reports to determine whether the adjustments to the receivable amounts were properly valued based upon actual revenues and expenditures **(Valuation)**.
- Year-end accrual - We plan to review all related year-end accrual JVs and their backup documentation for HCA and DSHS, including enterprise reporting reports, to determine whether the final accrual is properly valued based upon actual revenues and expenditures **(Existence and Valuation)**.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## **D.7.PR.G - Due From Other Governments**

*Procedure Step:* Substantive Test

*Prepared By:* EZM, 11/15/2024

# State of Washington

*Reviewed By:* RKM, 11/21/2024

## Purpose/Conclusion.

### Purpose:

To determine reported receivables represent amounts uncollected as of the end of the period  
To determine whether other assets were reported at properly valued or calculated amounts.

### Conclusion:

Reported receivable amounts represent amounts uncollected as of the end of the period. **No issues noted.**  
Receivable amounts were reported at properly valued and calculated amounts. **No issues noted.**

## Testing Strategy.

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

- Adjustments to Receivable balances - We plan to sample draw-down workbooks from HCA and review backup documentation including enterprise reporting reports to determine whether the adjustments to the receivable amounts were properly valued based upon actual revenues and expenditures (**Valuation**).
- Year-end accrual - We plan to review all related year-end accrual JVs and their backup documentation including enterprise reporting reports to determine whether the final accrual is properly valued based upon actual revenues and expenditures (**Existence and Valuation**).

## Guidance/Criteria.

## Record of Work Done.

### **Population Reconciliation Procedures for the Due from Other Governments Line Item** [JV Population Reconciliation]

We ran queries from the ACFR database for the significant balances (Rollup fund FAA and GL Sort Code CD) for HCA and DSHS.

We ran queries in Enterprise Reporting Web Intelligence which were filtered to match the results of the ACFR database to obtain transaction level detail for sampling. We reconciled the amounts by GL to the ACFR query with **no variances noted**. As the total population of the Webi queries' Due from Receivables reconciled to the ACFR database, we consider the transaction data to be complete.

# State of Washington

## **Sample Frame**

For both agencies, GL1351 (Due from Federal Government) composed the significant percentage of receivable amounts in the line item at year-end (95% for HCA and 87% for DSHS). Based upon this information, we elected to test only from this GL account. This is in line with our assumptions as these agencies participate in federal reimbursable programs (Medicaid primarily).

Per our understandings and testing strategy, we split the transactions into:

1. Adjustments to the GL1351 balance during FY24, and
2. The year-end accruals, identified by:
  - a. FM99/Current Doc MAJV8189 for HCA
  - b. Batch type KH for DSHS (batches in FM12 and 99)

## **Substantive tests performed to meet the Existence assertion**

### Testing Procedures:

Review all related year-end accrual JVs and their backup documentation including enterprise reporting reports to determine whether the final accrual is properly valued based upon actual revenues and expenditures.

**HCA:** [HCA YE Accrual]

**DSHS:** [DSHS YE Accrual]

We reviewed the year-end accrual JVs and the backup documentation including Enterprise Reporting reports (Revenue Accrual Calculation by Program/Account/Major Source/Source/Subsource) and e-mail correspondence. For each run of the year-end accrual, we recalculated the revenue accrual based upon subsource and compared them to recorded amounts ensure that a year-end receivable actually existed (expenditures exceeded revenues).

### Testing Results:

Year-end accrued federal revenues and the federal receivable actually existed as of year-end as the expenditures exceeded revenues for relevant subsources. **No issues noted.**

**No issues noted.**

## **Substantive tests performed to meet the Valuation assertion:**

### *Year-End Accrual*

### Testing Procedures:

Review all related year-end accrual JVs and their backup documentation including enterprise reporting reports to determine whether the final accrual is properly valued based upon actual revenues and expenditures

**HCA:** [HCA YE Accrual]



# State of Washington

## **DSHS:** [DSHS YE Accrual]

We reviewed the year-end accrual JVs and the backup documentation including Enterprise Reporting reports (Revenue Accrual Calculation by Program/Account/Major Source/Source/Subsource) and e-mail correspondence. For each run of the year-end accrual, we recalculated the revenue accrual based upon subsource and compared them to recorded amounts to ensure that a year-end receivable was correctly valued.

### Testing Results:

Year-end accrued federal revenues and the federal receivable was correctly calculated based upon FY expenditures and revenues for relevant subsources. **No issues noted.**

### *Adjustments to Receivables*

#### Testing Procedures:

We plan to sample draw-down workbooks from HCA and DSHS and review backup documentation including enterprise reporting reports to determine whether the adjustments to the receivable amounts were properly valued based upon actual revenues and expenditures and correctly calculated (**Valuation**).

We ran a query in Enterprise Reporting WEBi for the following query filters for fiscal year 2024:

- GL Account = 0159 (liability liquidations)
- Cost Allocation Funding Type = "F"

We summarized the liquidations by Process Date and Cost Objective and compared the totals of each cost objective in the liquidations report to the recorded adjustments to GL1351 in the draw calculation workbooks\* processed during sample drawdowns. We additionally recalculated the adjustment amount through a review of the drawdown's total draw and current draw amounts (based upon the current expenditures/revenues).

\*Note: Draw calculation workbook amounts for subsources for transaction codes 835. These transaction codes are associated with the liquidations of GL1351 receivable amounts. Total draws factor in current expenditures and revenues (GLs 6510/3210)

### Testing Results:

#### **HCA:** [HCA Due From Adjustments Testing]

#### **DSHS:** [DSHS Due From Adjustments Testing]

Adjustments to the federal receivable during drawdowns were properly valued and based upon prior period expenditure liquidations (GL0159). **No issues noted.**

# State of Washington

## E.1.PRG - Cash & Cash Equivalents

*Procedure Step:* Summary & Conclusion

*Prepared By:* DRR, 10/23/2024

*Reviewed By:* RKM, 11/20/2024

Purpose/Conclusion:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In

# State of Washington

making this determination, auditors should evaluate:

## Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the **Permanent File** folder or assessment of control risk?
  - If circumvention, the **Management Override of Controls** step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained is sufficient and appropriate.

## **E.1.PRG - Cash & Cash Equivalents**

*Procedure Step:* Understanding of Line Item

*Prepared By:* DRR, 5/20/2024

*Reviewed By:* RKM, 5/29/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associated with the line item.
- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

## State of Washington

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions:**

We noted one exit item related to this balance from the prior audit:

- The Employment Security Department (ESD) was unable to completely reconcile their bank accounts to the accounting records at fiscal year end June 30, 2023. Various reconciling items totaling \$(34,060,232) should not have been included in their respective reconciliations. We determined, after removing these reconciling errors from the reconciliations, that ESD understated Cash & Cash Equivalents by \$16,573,418.

As we will be reviewing the Departments bank reconciliations as part of our testing of this balance, we did not follow-up with Department staff regarding the Departments response or correction of this issue.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

We noted the balance included activity from the following funds:

- 620: Unemployment Compensation Account
- 622: Unemployment Compensation Federal Employees' Benefit Payment Account
- 22E: Family and Medical Leave Enforcement Account
- 22F: Family and Medical Leave Insurance Account
- 567: Long-Term Services & Supports Trust Account

We evaluated the funds and determined transactions from fund 620 make up most of the account balance. The Cash & Cash Equivalents line item

## State of Washington

is mainly composed of cash collected from employers, cash held for the minimum amount of operations (6-10 million), cash held in the trust fund, and cash ready to be expended for unemployment insurance benefits. The majority of the changes to this balance over the prior year were in fund 620 GL account 1150 "Cash with Fiscal Agents" and fund 620 GL account 1110 "Cash in Bank". This GL account 1150 increased \$676.5 million (25%) over the prior year and GL account 1110 decreased \$197 million (-62.5%). Overall this balance increased 15.6% from the prior year.

The Cash & Cash Equivalents line item is composed of three main cash accounts and two pandemic cash accounts that the ESD held during FY24. The Key Bank accounts discussed in the FY23 ACFR were closed in January 2024 and the funds in these accounts, if applicable, were rolled into their respective US Bank accounts. See below for ESD's current accounts:

- Main Accounts
  - US Bank Clearance Account (Employer Side)
  - US Treasury Trust Account
  - US Bank Benefit Account
- Pandemic Accounts
  - State Pandemic Relief Program (PRP) US Bank Account
  - Lost Wages Assistant (LWA) US Bank Account

### **(3) Updates to Significant Account Matrix:**

- None

### **E.1.PR.G - Cash & Cash Equivalents**

*Procedure Step:* Controls - Cash Reconciliations

*Prepared By:* DRR, 6/10/2024

*Reviewed By:* RKM, 6/11/2024

Purpose/Conclusion:
---------------------

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

# State of Washington

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable



## State of Washington

assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Significant Balance(s) and Assertions**

Internal controls in the Cash Reconciliation address the following balance(s):

- Statement of Net Position - Government Wide
  - Cash and Cash Equivalents
- Statement of Net Position - Proprietary Funds
  - Cash and Cash Equivalents (Local Portion)

For the following assertions:

- Existence
  - There is risk that reported cash and cash equivalents don't match reconciled bank accounts and records. In the prior audit we found an error in the cash reconciliation.

## **Gain an Understanding of Internal Controls**

We met with the following people on May 1, 2024 to update our understanding over cash and cash equivalents:

- Meghan Phelps, Treasury Manager
- Shelly Peterson, Assistant Treasury Manager
- Son Pham, Fiscal Analyst 4

Meghan Phelps, Treasury Manager, started her position in March 2024. Prior to March 2024, Aundrea Nunez, Controller, performed most reviews of the bank reconciliations while the Treasury Department transitioned between managers. The Employment Security Department (ESD) held three main cash accounts and two pandemic cash accounts during FY24. The Key Bank accounts previously used by ESD were closed on January

## State of Washington

19, 2024 and funds in these accounts were rolled into their new US Bank accounts. Cash accounts held with US Bank are managed under four master accounts. Sub-accounts are used to isolate transactions between receipts and payments. All sub-accounts are swept to the master account every night. Also, ESD held funds at the US Federal Treasury for the state and Federal Trust fund. Most cash is held with the Federal Treasury.

The general flow of funds consists of the following:

1. Cash is receipted in the clearance account. Payments are typically from employers for payment of their unemployment taxes. Funds in excess of operating needs are transferred into the Treasury Trust account.
2. Funds are held in the Treasury Trust account until needed.
3. Money is transferred out of the Treasury Trust and temporary accounts to the benefit account for payments to claimants for unemployment benefits.

State month end close occurs on the 10<sup>th</sup> business day of the following month. Reconciliations are performed shortly after (mid/end-month).

### US Bank Clearance Account (Employer Side)

The main purpose of the clearance account was to collect cash from employers, hold a minimum amount for operations, and remit all excess collected funds to the trust accounts held with the US Treasury in a daily transfer.

The clearance account consists of the following accounts:

1. Clearance Master
2. Clearance Disbursement
3. Clearance Deposit

Nightly, the clearance disbursement and clearance deposit accounts are swept into the clearance master account.

### Monthly Reconciliations for Clearance Accounts (Existence)

The banking desk prepares the clearance account reconciliation. My-Phuong Tran, Fiscal Analyst 3, prepares the reconciliation. She downloads the monthly statement from US Bank's online bank module. She downloads all three account statements and reconciles all three to ensure the existence of all cash transactions reported in the general ledger. Supporting documentation included "Monthly AFRS JV," GL balance from AFRS, and other reconciling items support as needed. My-Phuong signs the reconciliation and routes it to Meghan Phelps, Treasury Manager, or Shelly Peterson, Assistant Treasury Manager. Either Meghan or Shelly then electronically review the reconciliation and indicates reconciling items were accurate with tickmarks to ensure reported cash existed at year end (**Key Control 1 - Existence**). Meghan or Shelly then signs or initials the reconciliation to document the review.

### US Treasury Trust Account

ESD remits all excess cash to their US Treasury account. Excess limits are determined internally and based on cash needs. Based on minimum

## State of Washington

balances set in years prior, ESD determined \$6-10 million was the minimum balance needed to maintain operations. Minimums aren't expected to change.

The US Treasury account held the state and federal trust accounts. The US Treasury does not prepare traditional statements. In lieu of a monthly bank statement, Shelly Peterson, Assistant Treasury Manager, obtains three reports from TreasuryDirect.gov to verify the accuracy and existence of cash general ledger transactions. The three reports are:

1. Transaction Report: This report detailed all transactions by program.
2. Account Summary: This report detailed all transactions without classification of program.
3. Federal Report: The report detailed only federal program transactions.

Here is a link to the website that the ESD obtains the reports from: <https://www.treasurydirect.gov/govt/reports/tbp/account-statement/report.html>

Transactions (date, amount, classification) from the above reports are vouched to the Excel file "Monthly AFRS JV" workbook. Typically there are a few reconciling items (cash transfers between accounts that occurred before the bank's deadline). Shelly prepares the reconciliation from a template. Reconciliations are saved in Excel workbook "GL 1150 to Trust Fund". Reconciling items are typically for the last day of the trust fund draw and benefit returns for special programs like Federal Additional Compensation (FAC), Extended Benefit (EB), and Emergency Employment Compensation (EEC). Meghan Phelps, Treasury Manager, reviews the GL 1150 to Trust Fund reconciliation and supporting documentation, which includes Account Settlement Reports from ASAP.gov, reports from Treasury Direct, reports that show amounts sent to AFRS from their benefits payment system, and the Trust Fund Journal (**Key Control 1 - Existence**).

### US Bank Benefit Account

In general, the Benefit Account receives transfers from the US Treasury Trust Fund account. The Benefit account expends benefits to eligible participants. Trust Fund draws are based on UTAB report data of benefits paid to eligible participants for almost all benefit types. For more information on US Treasury Trust Fund draws, see our premiums and claims write up here [[Controls - UTAB](#)].

The master benefit account consists of the following accounts:

1. Benefit Master
2. Benefit Warrant Disbursement
3. Benefit ACH & Debit Card Disbursement
4. Benefit EFT
5. Benefit Deposit

### Monthly Reconciliations of Benefit Accounts (Existence)

Before state close and after UTAB sends the file (5<sup>th</sup> or 6<sup>th</sup> business day of the following month), Son Pham, Fiscal Analyst 4, pulls general ledger

## State of Washington

activity from AFRS (WEBI report) by fund (state benefits Fund 620 and federal benefits Fund 622). AFRS activity is entered into the "Monthly AFRS JV" Excel file. Activity from AFRS is reconciled to the "Monthly AFRS JV" Excel file. If any errors are found, JVs are used to correct the activity in the following month's activity. The accounting desk uses reports from UTAB and reconciles that to the AFRS JV spreadsheet monthly. After the monthly AFRS JV spreadsheet is reconciled then it gets reconciled to bank.

When the AFRS activity is reconciled to the "Monthly AFRS JV" Excel file, My-Phuong Tran, Fiscal Analyst 3, reconciles the five benefit account statements using a template. She also generates daily and monthly reports from UTAB (see list below) to aid in her reconciliation. Meghan Phelps, Treasury Manager, or Shelly Peterson, Assistant Treasury Manager, reviews the reconciliation and indicates reconciling items were accurate with tickmarks to ensure reported cash existed at year end (**Key Control 1 - Existence**). Meghan or Shelly then signs or initials the reconciliation to document the review.

Lastly, after state close (10<sup>th</sup> business day of the following month), Son pulls the same general ledger activity from AFRS by fund to ensure there were no changes.

Monthly UTAB Reports used in the Benefit Account Reconciliation:

1. Intercepted Money filtered for the month (benefits issued to claimant paid to another source for back taxes or child support)
2. UTAB Repayments (Details) filtered by source (US Bank Electronic Bill) and reason (returned payment)
3. UTAB Repayments (Details) filtered by source (lock box) and reason (returned payment)
4. General Ledger Posting filtered for cash draws related the end of the month and posted in the following month (dates depended on the month and business days)
5. General Ledger Posting filtered for book transfers related to the end of the month and posted in the following month (dates depended on the month and business days)

Daily UTAB Reports used in the Benefit Account Reconciliation:

6. Issued Funds (Benefit Payments & Refunds) filtered by payment channel (standard paper checks)
7. Issued Funds (Benefit Payments & Refunds) filtered by date (dates depended on the month and business days)

My-Phuong, Fiscal Analyst 3, uses a snippet of UTAB to support outstanding checks. The image is saved in the cash reconciliation workbook.

### Pandemic - US Bank Accounts

There are 2 pandemic US Bank accounts. Please see below:

- State Pandemic Relief Program (PRP) Account
  - This account was opened during December 2020 due to the extension of pandemic unemployment assistance (PUA) benefits not being signed in time by the federal legislation. Due to the extension not being signed, on December 27, 2020, Governor Jay Inslee authorized the use of federal CARES Act funds (approximately \$50 million) to help Washington claimants whose PUA

## State of Washington

benefits expired on December 26, 2020 and were waiting for federal legislation to extend those benefits. Federal legislation ended up getting signed into law on December 27, 2020, which extended, expanded, and changed the CARES Act provisions. Regardless, claimants eligible for the one-time PRP payment (\$550) still received it.

- Meghan stated that currently there a small amount left in this account.
- Monthly Reconciliation: This is similar to the reconciliation for the US Bank Benefit Account (see above), however there are no sub-accounts. Before state close and after UTAB sends the entry to AFRS (5<sup>th</sup> or 6<sup>th</sup> business day of the following month), My-Phuong Tran, Fiscal Analyst 3, prepares the bank to AFRS reconciliation, Meghan Phelps, Treasury Manager, or Shelly Peterson, Assistant Treasury Manager, reviews the reconciliation and indicates reconciling items were accurate with tickmarks to ensure reported cash existed at year end **(Key Control 1 - Existence)**. Meghan or Shelly then signs or initials the reconciliation to document the review.
- Lost Wages Assistance (LWA) Account
  - This account was opened by the ESD during August 2020 due to the ESD being approved for the LWA program through the Federal Emergency Management Agency (FEMA). LWA is a federal program that adds \$300 for each week the program remains federally funded. The ESD started processing LWA payments on September 21, 2020. Approved weeks for the program:
    - August 1 - 29, 2020
    - September 5, 2020
  - Department of Labor deposited the funds (approximately 708 million) from FEMA to their LWA account and the ESD was only able to draw down the funds based on what their actual draws were for the program.
  - They are currently receiving repayments in this account. This account has changed permanent account.
  - Monthly Reconciliation: This is similar to the reconciliation for the US Bank Benefit Account (see above), however there are no sub-accounts. Before state close and after UTAB sends the entry to AFRS (5<sup>th</sup> or 6<sup>th</sup> business day of the following month), My-Phuong Tran, Fiscal Analyst 3, prepares the bank to AFRS reconciliation, Meghan Phelps, Treasury Manager, or Shelly Peterson, Assistant Treasury Manager reviews the reconciliation and indicates reconciling items were accurate with tickmarks to ensure reported cash existed at year end **(Key Control 1 - Existence)**. Meghan or Shelly then signs or initials the reconciliation to document the review.

### How Transactions are Recorded in AFRS:

- Journal Entries: Journal entries were used to record cash received and transfers (i.e. from the Clearing Account to the US Treasury Trust Fund and from the US Treasury Trust Fund to the Benefit Account). Journal vouchers were also used to enter adjustments or corrections (Employer Side).
- System Interface: UTAB data posted to AFRS monthly in an automatic journal voucher.

### Key Controls are as Follows:

## State of Washington

- **Key Control 1:** The Treasury Manager or Assistant Treasury Manager review reconciliations and indicate reconciling items are accurate with tickmarks to ensure reported cash existed at period end **(Existence)**.

### Noted Weaknesses are as Follows:

- None

### E.1.PRG - Cash & Cash Equivalents

*Procedure Step:* Key Control 1 (Cash Reconciliations)

*Prepared By:* DRR, 6/5/2024

*Reviewed By:* RKM, 9/20/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm cash reconciliations were reviewed by the Treasury Manager or Assistant Treasury Manager **(Key Control 1 - Cash Reconciliations)** in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

## State of Washington

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*



## State of Washington

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done.:

### **Cash and Cash Equivalents - Existence**

# State of Washington

**Key Control 1 (Existence - Manual):** The Treasury Manager or the Assistant Treasury Manager review reconciliations and indicate reconciling items are accurate with tickmarks to ensure reported cash existed at period end.

The understanding for this system is documented above in the "Controls - Cash Reconciliations" step.

## **1. Confirmation of Key Manual Control:**

### **January 2024 Reconciliations:**

1. Clearance Master Account (account number ending in 9589)

US Bank Balance: \$51,418,218.64

Adjusted GL Balance: \$51,418,218.65

Variance: \$0.01

Preparation: We noted My-Phuong Tran, Fiscal Analyst 3, prepared this reconciliation.

Review: We noted Aundrea Nunez, Controller, signed off on the reconciliation to document her review. Additionally, we were provided with the January 2024 KeyBank statement for account 1184, which had a balance of \$2,608.01 and was closed on January 19, 2024, and deposited in account 9589 on January 31, 2024. **No issues noted.**

2. Trust Fund Account

Trust Balance: \$3,452,897,229.07

Adjusted GL Balance: \$3,441,830,952.17 (reconciling item of \$11,066,276.90 due to Last Day State Draw)

Variance: \$0.00

Preparation: We noted Shelly Peterson, Assistant Treasury Manager, prepared the reconciliation.

Review: We noted Aundrea Nunez, Controller, made tickmarks and signed off on the reconciliation to document her review. **No issues noted.**

3. Benefit Master Account (account number ending 9530)

US Bank Balance: \$71,705,597.46

US Bank Adjusted GL Balance: \$71,705,597.46

Variance: \$0.00

Preparation: We noted My-Phuong Tran, Fiscal Analyst 3, prepared the reconciliation.

Review: We noted Aundrea Nunez, Controller signed off on the reconciliation to document her review. Additionally, we were provided with the January 2024 KeyBank statement for account 3855, which was closed on January 19, 2024, and deposited in account 9548 on January 26, 2024. **No issues noted.**

See UTAB reconciliation at: [Key Control 6 (Manual - UTAB to AFRS Reconciliation)].

## State of Washington

### 4. State Pandemic Relief Program (PRP) Account (account number ending 9639)

US Bank Balance: \$1,360.00

Adjusted GL Balance: \$1,360.00

Variance: \$0.00

Preparation: We noted My-Phuong Tran, Fiscal Analyst 3, prepared this reconciliation.

Review: We noted Aundrea Nunez, Controller signed off on the reconciliation to document her review. Additionally, we were provided with the January 2024 KeyBank statement for account 0229, which was closed on January 18, 2024 and had a \$0 balance prior to closure. ***No issues noted.***

### 5. Lost Wages Assistance (LWA) Account (account number ending 9621)

US Bank Balance: \$3,890,344.10

Adjusted GL Balance: \$3,649,421.22 (reconciling items of \$240,922.88 due to transfers from 9530)

Variance: \$0.00

Preparation: We noted My-Phuong Tran, Fiscal Analyst 3, prepared this reconciliation.

Review: We noted Aundrea Nunez, Controller signed off on the reconciliation to document her review. Additionally, we were provided with the January 2024 KeyBank statement for account 8181, which was closed on January 18, 2024 and had a \$0 balance prior to closure. ***No issues noted.***

***No issues noted.***

Note: Prior to March 2024, Aundrea Nunez, Controller, performed most reviews of the bank reconciliations while the Treasury Department transitioned between managers.

### **Noted Weaknesses are as follows:**

- None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.1.PRG - Cash & Cash Equivalents**

# State of Washington

*Procedure Step:* Risk Assessment  
*Prepared By:* DRR, 6/18/2024  
*Reviewed By:* RKM, 9/30/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

## State of Washington

- *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*
- *Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*
- *Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*
- *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*
  - *Are there substantial pressures or motivations to misstate the balance?*
- *Inherent Risk due to Misappropriation*
  - *Is the account balance or transaction class susceptible to sizable misappropriation?*
- *Inherent Risk due to Non-Compliance*
  - *Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*
  - *Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*
  - *Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a

## State of Washington

combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- **Existence – HIGH**

# State of Washington

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

- **Cash Reconciliations** – Existence

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

- Existence – HIGH

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

- We do not plan to send cash confirmations to third parties. As an alternative, we plan to obtain month-end reports from TreasuryDirect.gov for the trust account. We expect the trust account to hold the majority of the Department's cash.
- We also plan to test cash reconciliations for other bank accounts (i.e. clearance, trust benefit, PRP, and LWA). We will test all reconciling items above the floor.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## **E.1.PRG - Cash & Cash Equivalents**

*Procedure Step:* Substantive Test  
*Prepared By:* DRR, 10/23/2024  
*Reviewed By:* RKM, 10/29/2024

# State of Washington

## Purpose/Conclusion:

### **Purpose:**

To determine whether reported cash and cash equivalents existed as of the end of the period **(Existence)**.

### **Conclusion:**

We determined cash and cash equivalents existed as of the end of the period, however, through testing we determined the following:

- We noted that there were several reconciling items in the benefit master account reconciliation that should not have been included. These reconciling items totaled \$(4,795,580) and resulted in an understatement of cash and cash equivalents by \$9,090,932. **See issue [E: ESD Cash Reconciliation Variances] and AOM [Aggregation of Misstatements (GAAP)].**

## Testing Strategy:

### **SAO Policy Requirement: Confirming or Verifying Cash & Investment Balances**

Confirmations can either be blind or a positive confirmation. In a blind confirmation (sweep), the auditor requests information on all accounts the bank holds for the entity (by entity name and/or EIN). In a positive confirmation, the auditor lists accounts (or accounts and balances) per the entity and asks the bank to confirm that the information is correct.

- Confirm cash and investment account balances with County Treasurer, bank and/or brokerage. Use the template confirmation form provided in the Store when needed.
  - Confirmations can be mailed to addresses listed on the Bank Confirmation Address List available on the Auditor Reference Guide. If the bank notifies you of a different address, please contact Team Audit Support to update the list.
  - Banks may confirm incorrect amounts either due to a simple mistake, use of a wrong confirmation date or incorrectly including or excluding accounts. The first step in resolving differences should be to check information against the entity's bank statements and then call the bank to specifically confirm any difference.
  - Confirming investments may involve physical inspection, confirmation with the issuer, confirmation with the custodian, confirmation of unsettled transactions with the broker/dealer, confirmation with the counterparty, and/or reading executed partnership or similar agreements. When confirming investments, ensure investments are held in the entity's name.
- *If confirmations are not used*, auditors must at minimum verify balances to the County Treasurer, bank and/or brokerage statements. If this is done, the auditor should consider the risk that the statements were altered and should examine papers for indications of alteration.

The following is a list of **additional considerations** for testing the existence assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.



# State of Washington

## Bank Reconciliations

If the auditor is comparing reconciled (confirmed) bank or county treasurer balances to the GL (rather than confirmed amounts within an expected variance due to reconciling items), the auditor should consider performing some or all of the following tests to verify the accuracy of the reconciliations. Note that testing the reconciliation will provide evidence of both the existence and completeness of cash and investment balances.

- Trace (or compare summed) bank balances per statements to reconciliations.
- Trace (or compare summed) book balances per reconciliations to the general ledger or financial statements.

*If a cash account is allocable to a particular fund, the balance in the general ledger should be recorded in the same fund.*

- Scan the reconciliation for reasonableness. Look for unusual, unexpected or vaguely described reconciling items, lack of support or detail, very large reconciling items, very old reconciling items, and missing or extra elements that would indicate that the reconciliation was being performed incorrectly.
- Foot the reconciliation for accuracy.
- Trace deposits in transit to the subsequent month's bank statement, considering reasonableness of the in-transit period.
- Trace outstanding checks to cash disbursement journal.
- Check that any other reconciling items are valid and have been properly accounted for (ex: large debit or credit memos).
- Check reconciliation against prior and/or subsequent reconciliations for reasonableness of amounts and items included and to trace reconciling items from the previous and/or subsequent period.

## Other Tests

- Inquire whether any checks or deposits were being held at year end for budget, cash flow or other purposes.
- Confirm investments purchased but not received as of year-end
- Confirm investments sold but still held as of year-end
- Confirm interest due or accrued but not yet received as of year-end
- Search for manual journal entries that debit (increase) cash. Consider testing if risk indicators are noted.
- Review reconciliations of clearing and transmittal accounts.
- See accountability steps for testing strategies related to petty cash and imprest funds, which are not expected to be material to the financial statements.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the*

# State of Washington

*government's deposits or investments.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Outstanding Checks and Deposits in Transit** – Per TIS section 1100.08 (AICPA Technical Questions and Answers), outstanding checks should be reported as a reduction of cash and the amount of deposits in transit should be reported as cash. A check is considered outstanding from the time that it is out of the payor's control – when mailed or delivered to the payee – until the time it clears the bank. Cash should represent amounts within the control of the reporting entity, that is, the amount of cash in banks plus cash and checks on hand and deposits in transit minus the amount of outstanding checks.

**SAO Audit Policy [6350](#) – External Confirmations**

**[Investments](#) Area Guide**

**[LGIP Fund Summary Reports](#)** - includes a list of local government accounts and balances in the Local Government Investment Pool

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.8.6](#) Use of Payroll and Claims Funds**

Record of Work Done:

## **Substantive tests performed to meet the Existence assertion**

We obtained the year-end reconciliations for the following accounts:

1. Trust Account held with the US Department of Treasury
2. Benefit Master Account held at US Bank and Key Bank
3. Clearance Master Account held at US Bank and Key Bank
4. Pandemic Relief Account held at US Bank
5. Lost Wages Assistance Account held at US Bank

See testing: [[Cash & Cash Equivalents Testing](#)]. We performed the following required and additional procedures:

# State of Washington

## Required Procedure:

### **1. Confirm cash and investment account balances with bank and/or brokerage.**

- We did not perform formal cash confirmations. We performed additional procedures noted below. During those procedures, we reviewed documentation for alterations or modifications. We did not note any alterations or modifications to any documentation. In addition to the procedures performed below, we obtained the Employment Security Department's (ESD) June 30, 2024 trust fund account statement from the U.S. Treasury's website, [TreasuryDirect](#).

## Additional Procedures:

### **1. Trace (or compare summed) bank balances per statements to reconciliations.**

- We vouched bank balances presented on each reconciliation to the respective bank statement. *No issues noted.*

### **2. Trace (or compare summed) book balances per reconciliations to the general ledger or financial statements.**

- We compared the bank reconciliation balances to the general ledger balances as reported in the ACFR database. See: [\[Cash & Cash Equivalents Testing\]](#), tabs, "Existence" and "Testing", for tying the general ledger balances as reported in the ACFR database to the financial statements. Through testing we determined the following:
  - We noted that several reconciling items in the benefit master account totaling \$(4,795,580), should not have been included in their respective reconciliations.
  - We determined that the Cash & Cash Equivalents balance was understated by \$9,090,932. **See issue and AOM link in the conclusion.**

### **3. Scan the reconciliation for reasonableness. Look for unusual, unexpected or vaguely described reconciling items, lack of support or detail, very large reconciling items, very old reconciling items, and missing or extra elements that would indicate that the reconciliation was being performed incorrectly.**

- We re-performed the ESD's cash reconciliations. We reconciled bank balances to the general ledger. We listed all reconciling items and descriptions at: [\[Cash & Cash Equivalents Testing\]](#), see tab, "Existence". We vouched all items greater than the floor to the source documentation. See tab "Testing". Through testing we determined the following:
  - We noted that several reconciling items in the benefit master account totaling \$(4,795,580), should not have been included in their respective reconciliations.
- We determined that the Cash & Cash Equivalents balance was understated by \$9,090,932. **See issue and AOM link in the conclusion.**

### **4. Foot the reconciliation for accuracy.**

## State of Washington

- We footed the reconciliations. We noted ESD's reconciliations of the Trust Fund, Clearance Master, Lost Wages Assistance, and Pandemic Relief accounts footed without exception. See: Cash & Cash Equivalents Testing, tab "Existence". ***No issues noted.***

**5. Trace deposits in transit to the subsequent month's bank statements, considering reasonableness of the in-transit period.**

- See procedure 3 above.

**6. Check that any other reconciling items are valid and have been properly accounted for (ex: large debit or credit memos).**

- See procedure 3 above.

**7. Check reconciliation against prior and/or subsequent reconciliations for reasonableness of amounts and items included and to trace reconciling items from the previous and/or subsequent period.**

- We reviewed cash testing from the FY 2023 ACFR to determine reasonableness. We determined the reconciliation was reasonable compared to prior year and found similar issues in the CY reconciliations.

### E.2.PRG - Receivables (Net of Allowance)

*Procedure Step:* Summary & Conclusion

*Prepared By:* DRR, 10/15/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion.:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy.:

# State of Washington

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?

## State of Washington

- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

Results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

# State of Washington

## E.2.PRg - Receivables (Net of Allowance)

*Procedure Step:* Understanding of Line Item

*Prepared By:* DRR, 6/11/2024

*Reviewed By:* RKM, 12/7/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associated with the line item.
- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and

## State of Washington

which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

We noted that the Employment Security Department (ESD) had the following three exceptions related to this balance in the fiscal year 2023 ACFR audit:

**(Finding)** ESD incorrectly calculated the allowance for doubtful receivables related to claimant overpayments. We found the allowance for uncollectible receivables related to claimant overpayments to be overstated and net receivables to be understated by \$330.5 million. This error was corrected in the financial statements.



# State of Washington

We recommend ESD perform a thorough review of the allowance for uncollectible receivables to ensure it is calculated correctly.

**(Verbal)** ESD is unable to fully reconcile receivables reported within UTAB to amounts reported within AFRS. The variance identified was \$548,531.

We recommend ESD to fully reconcile receivables reported within UTAB to AFRS.

**(Verbal)** The certified uncollectible amount (CUA) used to calculate the NGTS allowance was based on incomplete data. From 2018 to 2021 the CUA has been significantly higher. We were unable to quantify the understatement, however we don't expect this error to have a significant financial impact since the Department uses a five year average for their allowance estimate.

We recommend the Department to ensure complete date is used in their allowance methodology.

As we will be reviewing receivables and allowance for doubtful receivables during our testing, we did not inquire how the Department responded, or corrected the issue.

## **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

We noted the balance included activity from the following funds:

- 620: Unemployment Compensation Account
  - OFM Account description: The first priority is to provide services to eligible participants within the state; second priority is to provide substitute services or program support; and last priority is the direct payment of funds to the federal government.
    - Authority: RCW [50.16.010](#)
- 622: Unemployment Compensation Federal Employees' Benefit Payment Account
  - OFM Account description: Local fund outside the state treasury used to account for funds received from the federal government to cover benefits paid by the state for eligible unemployed federal workers. Per the Federal Employment Security Act (Title V).
    - Authority: RCW [43.88.195](#)

We evaluated the funds and determined transactions from fund 620 and 622 make up 74% of the account balance. The Receivables (Net of Allowance) line item is mostly composed of the receivables from employers (NGTS - taxes) and claimants (UTAB - overpayments).

We also identified that many of the funds did see some significant changes year over year (FY2022 to FY2023):

## State of Washington

- 620: Unemployment Compensation Account:
  - GL1342 (Accounts receivable) decreased by 21% or \$1M.
  - GL1349 (Allowance for Uncollectible Other receivables) increased by 14% or \$30M.

Fund 622 - Unemployment Compensation Federal Employees' Benefit Payment Account did not see significant changes from the prior year.

We inquired with Meghan Phelps, Treasury Manager, on May 23, 2024 and she stated that there were no significant changes from FY23 to FY24 in regards to the receivables (net of allowance) line item processes or procedures in the Treasury department, however, she noted that the agency is still applying federal waivers to some assessed over payments that occurred during the pandemic between February 2, 2020 and September 4, 2021.

On November 27, 2024 we inquired with Meghan Phelps, Treasury Manager, and Corbin Foster, Enterprise Financial Recovery Manager, to determine why the receivables balance is so large now, compared to pre-pandemic. Per Meghan, the reason for the increase in the balance is due to outstanding fraud benefits that were paid out during 2020 and 2021. Meghan stated that ESD has collected approximately \$450 million of the \$640 million that was paid out and ESD is still actively working with financial institutions and law enforcement to collect as much of the outstanding balance as possible. Per Meghan, she expects a more significant drop in FY25 as the Department continues it's overpayment waiver project and she would expect the backlog of collections to catch up over the next few years.

Corbin mentioned that during 2020 and 2021 the agency saw a dramatic increase in the overall volume and dollar amount of benefits paid out. He mentioned that during an 18 month period, ESD paid out the same amount of benefits from the previous 18 years. Additionally, he stated that "In the early days of the pandemic, agency leadership at the time decided to pause active collections, meaning for example the filing of liens against individuals and employers, the garnishing of assets such as wages or bank accounts, and proactively contacting customers to request payment. Throughout these past several years, we have allowed and welcomed customers who contact us to voluntarily remit payment or enter into long-term payment plans, and we have also continued offsetting benefits against any overpayment balances. The collections pause was lifted for employers in December 2023, and we are in the early stages of doing the same for UI claimants with benefit overpayments."

In Unemployment Insurance Program Letter Number (UIPL) 20-21, Change 1, U.S. Department of Labor provided scenarios where certain CARES Act overpayments may be waived on a blanket basis. This allows states to process waivers for multiple overpayments simultaneously based on a single set of facts that satisfy the requirement that the individual be without fault in the creation of the overpayment and that recovery would be contrary to equity and good conscience. UTAB has been automated to identify and process blanket waivers in the limited scenarios described in the UI Policy Update from February 14, 2023 found here [[UI Policy Update \(Including Fed. Waivers\)](#)].

The first round of these waivers were applied at the end of March 2023, with automatic waivers and write-offs to specific types of overpayments. There is an overpayment waiver request form on the ESD website that can be submitted by those assessed with overpayment notices and these are being manually reviewed by ESD staff to determine if the claimant is eligible for the waiver.

# State of Washington

**Note:** Federal Waivers were selected for audit in the FY23 Accountability audit of ESD at **[S1EmploymentSecurity-AC23]**. This work provides a complete understanding of the federal waiver process and has determined that the Department's methodology for applying waivers is correct.

## **(3) Updates to Significant Account Matrix:**

- None

## **E.2.PRG - Receivables (Net of Allowance)**

*Procedure Step:* Controls - UTAB

*Prepared By:* DRR, 10/11/2024

*Reviewed By:* RKM, 11/20/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.

## State of Washington

- Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
- Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
- Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.
- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

## State of Washington

- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

# State of Washington

## Record of Work Done:

Internal controls in UTAB address the following balances:

- Statement of Net Position - Proprietary Funds
  - Receivables (net of allowance)
- Statement of Net Position - Government Wide
  - Other Receivables (net of allowance for uncollectible)

For the following assertions:

- **Existence:** There is a risk that reported insurance premium receivables do not represent valid uncollected amounts due from employers and claimant overpayments and/or fraudulent payments at year end (Existence). There is as risk that federal waivers were included in the receivable balance (Existence - Significant Risk).
- **Valuation:** There a significant risk that a reasonable allowance for uncollectible accounts has not been established. There was an error (\$330.5M) in calculating the year-end adjustment for the UTAB allowance, which is an estimation performed at year-end (Valuation - Significant Risk).

### **Gain an Understanding of Internal Controls**

We met with the following people on May 23, 2024 to update our understanding over UTAB receivables:

- Meghan Phelps, Treasury Manager
- Shelley Peterson, Assistant Treasury Manager
- Son Pham, Fiscal Analyst

### **General Information:**

Claimant over-payments are tracked in GL 1319 and tracked by fund (620 – federal or 622 – state).

Over payments were governed by the following:

- RCW 50.20.190 - Recovery of benefit payments (<http://app.leg.wa.gov/rcw/default.aspx?cite=50.20.190>)
- WAC 192-220-045 - How is the fraud penalty calculated? (<http://apps.leg.wa.gov/wac/default.aspx?cite=192-220-045>)
- RCW 50.24.200 - Charge-off of uncollectible accounts (<https://app.leg.wa.gov/rcw/default.aspx?cite=50.24.200>)
- RCW 50.32.020 - Filing of benefit appeals (<https://app.leg.wa.gov/rcw/default.aspx?cite=50.32.020>)
- SAAM 85.54.55 – Receivables (<https://www.ofm.wa.gov/sites/default/files/public/legacy/policy/85.54.htm>)

### **Overpayment Penalties and Interest (UTAB Receivable)**

See understanding of UTAB benefits (Premiums & Claims) at: [[Premiums and Claims](#)]

## State of Washington

Over payments of unemployment benefits occur when someone received benefits that they are later found to have been ineligible to receive. This can happen if someone receives more benefits than they were entitled to. For example:

- A claimant was paid on a conditional basis while their case was under review and the review subsequently finds that they were not entitled to receive benefits.
- A claimant does not respond to requests for more information during a 10 day window. Benefits will stop and the amount already paid out will be due back to ESD.

Claimants are able to appeal and provide the requested information which, if approved, will negate the overpayment assessment letter.

When over payments are identified, the Department mails the claimant an overpayment assessment letter which details the amount of the overpayment and states that the claimant has 30 days to appeal the overpayment determination or provide additional information to the Department. Over payments were also classified as fraudulent and non-fraudulent.

### **Repayment of Over payments**

When over payments are identified, benefit recipients are not expected to repay the full amount due immediately. UTAB calculates the minimum monthly payment depending on the type of overpayment (fraud or non-fraud). The calculation is:

#### Fraud:

- The weekly benefit amount client was receiving at the time the overpayment occurred, or 3% of the overpayment balance, whichever is greater.
- Interest is assessed at 1% per month on the balance, the interest begins the day the overpayment is established.

#### Non-Fraud

- One third of the weekly benefit amount, 3% of the overpayment balance, or \$25.00, whichever is greater.
- Interest is assessed at 1% per month on the balance, on accounts at least a portion of two payments past due.

If the account is delinquent, UTAB calculates the minimum monthly payment by totaling the minimum monthly payment, accrued interest and past due amount.

When a client has an existing overpayment and begins claiming benefits, offsetting the principal balance will occur when:

1. The account is at least a portion of two payments past due; or
2. The overpayment is due to a UI Claim cancellation; or
3. The overpayment balance equals the New Balance Available (NBA) left on the UI Claim

Benefits will be offset at 50% of the weekly benefits payable for each week claimed for Non-Fraud over payments.

## State of Washington

Offsetting occurs at 100% of the weekly benefits payable for each week claimed for the following:

1. Fraud Over payments; or
2. The overpayment is due to a UI Claim cancellation; or
3. The overpayment balance equals the NBA left on the UI Claim

If the client sends in the full overdue amount, current monthly payment, and total interest owed to bring the account current, offsetting will stop as long as the client continues to keep the account current.

### **Monthly Review of UTAB Receivable Data (Existence/Valuation)**

UTAB automatically posts accounts receivable activity to AFRS monthly (6<sup>th</sup> business day after the end of the month). Activity is posted in summary. To review the automatic post, Son Pham, Fiscal Analyst 4, runs a general ledger query from the Web Intelligence (WEBI) system. The report is exported into an Excel workbook titled "New AFRS File," tab "Receivable Activity." Son takes a screen shot of the UTAB report titled "Aging Receivables", as of the last day of the month. She pastes the UTAB screen shot in the New AFRS File Excel workbook tab "Receivable Activity". Son ties totals from the UTAB aging report to the general ledger. If exceptions are noted, the Fiscal Analyst 4 prepares an adjusting journal voucher. When complete, Son notifies Shelly Peterson, Assistant Treasury Manager, and Meghan Phelps, Treasury Manager. Shelly or Meghan review the Excel workbook "New AFRS File" to ensure the receivables post from UTAB is accurately calculated, and receivables exist (**Key Control 1 – Manual - Existence/Valuation**).

The process described above is the same process for fraud receivables.

### **Calculation of Allowance for Doubtful Accounts (Valuation, Manual)**

The allowance for doubtful accounts estimate is prepared from historical receipt trends tracked in UTAB. Monthly, Meghan Phelps, Treasury Manager, reviews repayments by revenue source and aging. The UTAB report is called "Age of Account Payments," and documented in the Excel workbook "AgeOfAccountPayments\_YrEnd." The aging report is broken out by the following increments: 0-90 days, 91-180 days, 181-365 days, 366-730 days, 731-1,095 days, and 1,096 and more days. Collection percentages are calculated by dividing the total receipts for each aging bucket by the total receipts collected. Monthly percentages for each aging bucket are averaged to determine the collection percentages for the fiscal year. This is calculated on tabs "age of accounts (Fiscal Year)" and "Historical Percentage" in the AgeOfAccountPayments\_YrEnd workbook. The percent calculations are later used to estimate how much would be collected and how much would likely be written off.

Balances that were past due are tracked in the UTAB report "Uncollectible Balances." The Uncollectible Balances report tracks all repayment plans that are delinquent for 180 days or more. This report does not track the age of the initial repayment plan, but status of the repayment plan. Shelly Peterson, Assistant Treasury Manager, multiplies the total uncollectible balances by the annual average collection percentages for each respective aging bucket. This is calculated on tab "Quick Glance" in the AgeOfAccountPayments\_YrEnd workbook. The difference between the total uncollectible balances from the UTAB report and the expected repayment by aging category was the expected and likely write-off



## State of Washington

amount.

The uncollectible multiplying factor is determined by dividing the expected write off amount by total receivables (Age of Account Payments UTAB report). The multiplying factor is updated annually to reflect current collection practices and historical trends as calculated by the expected write-offs.

Shelly prepares a journal voucher based on the Excel workbook. Meghan Phelps, Treasury Manager, reviews and approves the journal voucher. She reviews the Excel formulas to ensure amounts were accurately calculated (**Key Control 2 – Valuation, Manual**). See below for GL coding (reversing JV):

- State (Fund 620) GL 1349/6505
- Federal (Fund 622) GL 1349/5151

Meghan also reviews the total allowance for doubtful accounts and the allowance as a percentage to total accounts receivable to determine consistency and reasonableness.

For fraud receivables they take the total UTAB receivables and determine what portion is related to fraud. They reduce the fraud receivable amount by any items still in process as of June 30, 2024. This amount is divided by the receivables amount to determine the percentage that will be determined uncollectible. The journal voucher preparation and review process is the same as described above.

We agree with ESD's methodology for determining allowance for doubtful accounts.

### Charge Off Criteria

UTAB automatically writes off balances (daily and yearly write-offs). Daily, UTAB reviews receivables and charged off balances that met the following criteria:

- Amounts less than \$25.00;
- No payment has been received within the past six months;
- The claimant did file or opened a claim within the last three months;
- If a lien was attached to the determination, the system automatically released the lien and sent notification to the county.

UTAB also reviews receivables annually and writes off balances that met the following criteria:

- Over payments were ten years or older or the overpayment was less than \$100 (total includes principal, penalty, interest, court cost, and surcharge);
- No repayments were made within the last 15 months;
- If a lien was attached to the determination, the system automatically released the lien and sent notification to the county.

## State of Washington

The annual review excludes over payments that were in suspense (by ESD, the business, stay of collection, prosecution, or request from the attorney general), out of state over payments, and balances greater than \$0 for current ESD employees.

### How transactions are recorded in AFRS:

- Accounts receivable data (monthly) is automatically posted to AFRS on the sixth business day after month-end.
- Year-end accounts receivable balances and related allowance for uncollectible accounts are posted to AFRS via journal voucher.

### Key Controls are as Follows:

- **Key Control 1 (Manual - Existence/Valuation):** Monthly, the Treasury Manager and Fiscal Analyst 4 review the Excel workbook "New AFRS File" (GL query run through WebI), tab "Aging Receivables" to ensure accounts receivable (including fraud) recorded in UTAB were accurately calculated, receivables existed and were correctly imported into AFRS from UTAB.
- **Key Control 2 (Manual - Valuation):** The Treasury Manager reviews and approves the JVs and related support to ensure the allowance for doubtful accounts (including fraud) was accurately calculated based on historical collection data and the correct percentage.

### Noted Weaknesses are as Follows:

- None

### E.2.PR.G - Receivables (Net of Allowance)

*Procedure Step:* Key Control #1 UTAB (Manual)

*Prepared By:* DRR, 6/25/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:
---------------------

### **Purpose:**

To confirm the Treasury Manager reviews the "New AFRS File" to ensure accounts receivable (including fraud) are accurately calculated and imported into AFRS from UTAB (**Key Control #1 for UTAB**) in order to assess control risk.

# State of Washington

## **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

## State of Washington

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

## **Receivables (Net of Allowance) (Existence/Valuation)**

**Key Control 1 (Existence/Valuation - Manual):** Monthly, the Treasury Manager and Fiscal Analyst 4 review the Excel workbook "New AFRS File" (GL query run through WebI), tab "Aging Receivables" to ensure accounts receivable (including fraud) recorded in UTAB were accurately calculated, receivables existed and were correctly imported into AFRS from UTAB.

The understanding for this system is documented above in the "Controls - UTAB" step.

### **1. Confirmation of Key Manual Control:**

We obtained the "New AFRS File March 2024" excel spreadsheet from Meghan Phelps, Treasury Manager. There was a tab in the spreadsheet titled, "Receivable Activity". This tab included the March 2024 Webi "Agency Wide Management Report by Date" (process date 4/16/2024). On this report, GL 1319 "other receivables" totaled \$10,890,305.04 in funds 620 and 622. GL 1349 "Allowance for uncollectible other receivables" was \$10,178,894.29 for funds 620 and 622. There was detail below which indicated the GL1319 and 1349 February ending balances, and the March ending balance after the adjustments noted above from the WEBi report.

Below that, there was a reconciliation of these balances to the adjustments from the UTAB report. There was a variance of \$2,252,630.22 in GL 1319 and the variance in GL 1349 was zero.

	GL1319	GL1349
Feb. Ending Balance	1,542,438,180.32	(1,478,476,529.38)
March Adjustment	10,890,305.04	(10,178,894.29)
<b>Total:</b>	1,553,328,485.36	(1,488,655,423.67)
UTAB	(1,572,288,942.45)	1,488,655,423.67

## State of Washington

Excess Repayment	16,707,826.87	-
Variance	(2,252,630.22)	-

We inquired with Meghan Phelps, Treasury Manager of the receivables variance, and she informed us that the variance is attributed to timing differences. These variances are reviewed, but not adjusted monthly. The main adjustment process is done at year end to calculate the allowance adjustment, which will be reviewed and confirmed for key control 2.

Below that, there were screen shots of UTAB reports providing support for the amounts used to reconcile the WEBI report to UTAB.

- The screen shot of the UTAB "Aging Receivables-details" report ending 3/31/2023 totaled \$1,572,288,942.45. This was composed of 8 years of receivables beginning in 2017. The revenue types were broken out and listed as "Receivable Fraud Open Balance (Uncollectible debt)", Receivable Interest Open Balance, Receivable Interest Open Balance (Uncollectible Debt), Receivable Penalty Open balance, Receivable Penalty Open Balance (Uncollectible Debt) ,Receivable Principal Open Balance, and Receivable Principal Open Balance (Uncollectible debt).
- The screenshot of "Aging Receivables-details" report for the Revenue Type - Excess Repayment (Repayment Balance) was composed of 8 years of receivables beginning in 2017 and totaled \$16,707,826.87.
- Another screen shot was included that broke down the Uncollectible Balance of \$1,488,655,423.67 by activity and revenue type: Fraud, Interest, Penalty, or Principal.

### **Noted Weaknesses are as follows:**

- None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.2.PR.G - Receivables (Net of Allowance)**

*Procedure Step:* Key Control #2 UTAB (Manual)

*Prepared By:* DRR, 10/16/2024

# State of Washington

Reviewed By: BM2, 11/20/2024

## Purpose/Conclusion.

### **Purpose:**

To confirm the Treasury Manager reviews and approves the JVs and related support to ensure the allowance for doubtful accounts (including fraud) was accurately calculated based on historical collection data and the correct percentage.

**(Key Control #2 for UTAB)** in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls, however, we did note the following:

- ESD's review of the UTAB allowance calculation was insufficient to ensure that the calculation was performed correctly. This resulted in an overstatement of GL1349 "Allowance for Uncollectible Other Receivables" for Funds 620 and 622 by \$5,455,650 and an equal understatement of GL1319 "Other Receivables" for Funds 620 and 622. **See issue:** [E: ESD UTAB Allowance Calculation Error]

## Testing Strategy.

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

## State of Washington

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it*



## State of Washington

*would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Receivables (Net of Allowance) (Valuation)**

**Key Control 2 (Valuation - Manual):** The Treasury Manager reviews and approves the JVs and related support to ensure the allowance for doubtful accounts (including fraud) was accurately calculated based on historical collection data and the correct percentage.

The understanding for this system is documented above in the "Controls - UTAB" step.

#### **1. Confirmation of Key Manual Control:**

We obtained journal vouchers and related support for the year end UTAB allowance for doubtful accounts adjustment. Meghan Phelps, Treasury Manager, prepared the JVs on 9/3/2024. Kim Green, Deputy CFO, reviewed and approved the JVs on 9/3/2024. The JVs were uploaded by Son Pham, Fiscal Analyst, on 9/3/2024 and released by Meghan Phelps on the same date.

## State of Washington

We received a spreadsheet titled "FY 2024 UTAB Allowance and Reversal" which included the journal entries, calculations performed and related support to book the allowance adjustment to GLs 1319 and 1349, which distinguished between fraud and non fraud receivables in funds 620 (state) and 622 (federal). There were numerous screen shots from the UTAB system of cube reports run on 8/13/2024 included as support for the numbers used in the calculation. Additionally, there were screen shots of ER General Ledger Trial Balance reports included as support for amounts used in the calculations.

Note: The percentage used to book the non-fraud allowance was identified as 32% (rounded) and the percentage used to book the fraud allowance was identified on the support as 97%.

- We were also provided with historical data from UTAB used to obtain the percentage used in the calculation, and we requested this information in excel to use for our testing.

We determined that the agency is using historical data and system reports to calculate the amounts for the journal entries to record allowance adjustments, and that these journal entries are reviewed and approved by ESD management prior to upload and release by ESD staff. However, we noted during our review and recalculation of the UTAB allowance [Allowance for Doubtful Accounts Testing - UTAB] that ESD referenced the FY23 multiplying factor, and not the FY24 multiplying factor when calculating their UTAB non-fraud allowance for doubtful accounts which resulted in an error of \$5,455,650. **See issue in conclusion above.**

### **Noted Weaknesses are as follows:**

- ESD's review of the UTAB allowance calculation was insufficient to ensure that the calculation was performed correctly. **See issue in conclusion above.**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.2.PR.G - Receivables (Net of Allowance)**

*Procedure Step:* Controls - NGTS

# State of Washington

*Prepared By:* DRR, 7/24/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.
- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.
- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

## State of Washington

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- *Initiation:* How are transactions initiated?
- *Authorization:* How are transactions and accounting record maintenance authorized?
- *Recording:* How are transactions or balances identified and recorded in financial accounting systems?

## State of Washington

- *Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- *Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls in NGTS address the following balances:

- Statement of Net Position - Proprietary Funds
  - Receivables (net of allowance)
- Statement of Net Position - Government Wide
  - Other Receivables (net of allowance for uncollectible)

For the following assertions:

- **Existence:** Reported insurance premium receivables do not represent valid uncollected amounts due from employers and claimant overpayments and/or fraudulent payments at year end.
- **Valuation:** There is a risk that a reasonable allowance for uncollectible accounts has not been established.

**Gain an Understanding of Internal Controls**

# State of Washington

We met with the following people on May 23, 2024 to update our understanding over NGTS receivables:

- Meghan Phelps, Treasury Manager
- Shelley Peterson, Assistant Treasury Manager
- Son Pham, Fiscal Analyst

## Source of Guidance

- Penalties for Late Reports and Contributions: [RCW 50.12.220](#)

## General Accounts Receivable Information - NGTS

Employers file quarterly hour and wage information for their respective employees. Reports are due one month after the end of the calendar quarter (i.e. April, July, October, and January). Accounts receivable statements are mailed monthly for balances greater than \$5.00.

## Basic Tax Calculation

Receivable balances are based on payroll data provided by employers and the employers respective unemployment tax rates as reported on quarterly tax reports. Reports are typically prepared online through the Next Generation Tax System (NGTS) and Employment Account Management Services (EAMS). The calculation is automatically calculated through the online reporting system. Tax rates are determined annually in the fall and notices are mailed to employers in December.

Rates are based on industry rates for new employers and historical information for established employers. Calculations for established employers comprised of the following:

- Unemployment Insurance Tax (Includes Social Cost)
- Employment Administrative Fund Tax

For a full understanding of premiums & assessments and related control confirmation see: [\[Premiums and Assessments\]](#).

## Accounts Receivable Monthly and Year-End JVs (Existence/Valuation, Manual)

Accounts receivable balances, employer account activity, and payments are managed in NGTS. NGTS receivable information is dynamic and does not produce historical information on reports. As such, the Treasury Department use and review a monthly SQL query to post and report accounts receivable. Query results are saved in an Excel workbook called, "Monthly NGTS Receivables". Query results are summarized by employer class in a pivot table. Query totals are reduced by amounts reported in future periods (all employer classes who reported amounts not due yet) and select employer class codes, such as, 154 - Federal Agencies and 155 - Military which is excluded because they are reimbursable employers, and ESD draws down funds through IB6 electronic billing process daily and payments do not get posted to NGTS. As ESD gets reimbursed daily for these employer class codes, there is no receivable related to them.

NGTS has an AR report that they compare to the SQL query. They do this monthly.

## State of Washington

Journal vouchers book the incremental change to the AFRS receivable balance. Adjustments are made to increase or decrease accounts receivable GL 1312 with an off-set to accrued revenue. The transaction code used to increase receivables and increase accrued revenue is 012 (GL 1312/3205). The transaction code used to decrease receivables and decrease accrued revenue is 020 (GL 3205/1312). The monthly journal vouchers are typically prepared by Son Pham, Fiscal Analyst 4, and reviewed by the Treasury Manager, or Assistant Treasury Manager to ensure receivables were calculated correctly and existed (**Key Control 1 - Manual - Existence/Valuation**).

The Employment Security Department (ESD) also uses additional queries to record period-end or year-end receivables. These receivables are for Q2 assessments (April - June) that are determined or estimated after June. See below for the queries used and a brief description:

1. Added: Second Quarter Assessments:

- This query is ran to capture assessments due for the second quarter (April-June) and due July 31st on the employer's quarterly report. This query is ran at the end of August (day before phase 2 close) to allow for as many employers as possible to complete their reporting and reduce ESD calculated assessments. This report is re-ran in late September or early October to ensure no significant changes of assessments as reported by employers reporting wages and hours.

2. Subtracted: Second Quarter Assessments Paid in June:

- This query lists all employers that filled and paid their second quarter assessments before fiscal year-end. Since payment is made prior to year end, ESD removed this from their receivable balance.

3. Added: Estimated Assessment for Second Quarter Based on First Quarter Return Data (wages and hours):

- This query is ran at the end of August (day before phase 2 close) to reduce the amount of estimated assessments. NGTS automatically calculates assessments for employers who reported wages in the first quarter of the year (January - March), but did not report wages for the second quarter (April - June).

4. Added: Estimated Assessments for Second Quarter not Previously Liabile:

- This query estimates the number of new employers who did not establish an employer account or file any quarterly returns. These estimates are based on the employer's industry average unemployment insurance tax. The number of estimated new employers is based on the previous year's actual new employers. Estimated new employers are charged the average filling amount. The average filling amount is determined by the Labor Market and Performance Analysis (LMPA) department.

Query results are summarized by employer class in a pivot table. Query totals are reduced by amounts reported in future periods (all employer classes who reported amounts not due yet) and select employer class codes, such as, 154 - Federal Agencies and 155 - Military which is excluded because they are reimbursable employers, and ESD draws down funds through IB6 electronic billing process daily and payments do not get posted to NGTS. As ESD gets reimbursed daily for these employer class codes, there is no receivable related to them.

## State of Washington

Adjustments are made to increase or decrease accounts receivable with an off-set to accrued revenue. The transaction code used to increase receivables and increase accrued revenue is 012 (GL 1312/3205). The transaction code used to decrease receivables and decrease accrued revenue is 020 (GL 3205/1312). Year-end journal vouchers are prepared by Shelly Peterson, Assistant Treasury Manager, and reviewed by Meghan Phelps, Treasury Manager to ensure receivables were calculated correctly and existed as of month and year-end (**Key Control 1 - Manual - Existence/Valuation**).

### Allowance for Doubtful Accounts Year-End Adjustments (Existence/Valuation, Manual)

The Department reviews allowance for doubtful accounts by reviewing revenues, collections, and write-offs. They expect the allowance for doubtful accounts to reflect the Department's actual write-offs. ESD calculates the allowance using the following queries:

- Query 1: Write-Offs Totals (CUA) – Annual with Average
  - The first query produces the amounts determined (certified) uncollectible by fiscal year. The report also aggregates annual uncollectible balances and produces the average yearly uncollectible amount. ESD uses a five year average. The five year average is considered as the basis for the allowance for doubtful accounts.
- Query 2: Detailed Write-Offs
  - The second query provides all the detailed write offs to ensure the accuracy of the annual query amounts. Amounts and assessment types are reviewed to ensure the average write-off amounts included NGTS related transactions. The query details the following information:
    - ESD Number
    - Legal Business Name
    - Transaction Date
    - Payment Method
    - Assessment Type
    - Write-Off Applied To (Account Where Write-Off Was Applied)
    - ASM Amount
    - CUA (Certified Uncollectible Amount)
    - Qtr/Year (When the Tax Assessment Was Earned)
    - Class (ESD Employer Class)
    - Ownership Structure
    - Transaction Type

If there is anything questionable in these queries Shelly or Meghan reach out to the NGTS team.

Son Pham, Fiscal Analyst 4, aggregates the results in an Excel workbook called "NGTS Allowance Calculation Template.xlsx". Adjustments are made to increase or decrease allowance for doubtful accounts with an off-set to accrued revenue. The transaction code used to increase the



## State of Washington

allowance for doubtful accounts and decrease accrued revenue is 122 (GL 3205/1342). The transaction code used to decrease allowance for doubtful accounts and increase accrued revenue is 122R (GL 1342/3205). The journal voucher is prepared by Son and reviewed by Shelly Peterson, Assistant Treasury Manager, or Meghan to ensure the estimate calculation reflected operations and historical trends (**Key Control 2 - Manual - Existence/Valuation**).

### How transactions are recorded in AFRS:

- Transactions are recorded in NGTS. NGTS data is queried and recorded in AFRS monthly and at year end by general journal vouchers prepared by Son Pham, Fiscal Analyst 4, and reviewed by Shelly Peterson, Assistant Treasury Manager.

### Key Controls are as Follows:

- **Key Control 1 (Manual):** Monthly, the Treasury Manager or Assistant Treasury Manager reviews journal vouchers to record the incremental change to the NGTS accounts receivable balance. The Assistant Treasury Manager reviews the monthly schedule of accounts receivable prepared by the Fiscal Analyst and supporting query results to ensure receivables were calculated correctly and existed (**Existence/Valuation**).
- **Key Control 2 (Manual):** The Treasury Manager or Assistant Treasury Manager reviews journal vouchers to record the incremental change to the allowance for doubtful accounts. The Treasury Manager reviews the quarterly Allowance for uncollectible accounts receivable schedule prepared by the Fiscal Analyst and the supporting query results to ensure the estimate calculation reflected operations and historical trends (**Existence/Valuation**).

### Noted Weaknesses are as Follows:

- None

### E.2.PRG - Receivables (Net of Allowance)

*Procedure Step:* Key Control #1 NGTS (Manual)

*Prepared By:* DRR, 6/25/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:
---------------------

### **Purpose:**

To confirm the Treasury Manager, or Assistant Treasury Manager reviews the monthly schedule of accounts receivable prepared by the Fiscal

## State of Washington

Analyst and supporting query results to ensure receivables were calculated correctly and existed (**Key Control #1 for NGTS**) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision,*

## State of Washington

*the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially*

## State of Washington

*be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Receivables (Net of Allowance) (Existence/Valuation)**

**Key Control 1 (Existence/Valuation - Manual):** Monthly, the Treasury Manager or Assistant Treasury Manager reviews journal vouchers to record the incremental change to the NGTS accounts receivable balance. The Assistant Treasury Manager reviews the monthly schedule of accounts receivable prepared by the Fiscal Analyst and supporting query results to ensure receivables were calculated correctly and existed

The understanding for this system is documented above in the "Controls - NGTS" step.

#### **1. Confirmation of Key Manual Control:**

We requested and obtained the "FUND 620 AR JULY 2023-JUNE 2025" excel spreadsheet and the journal voucher to record the incremental change to the NGTS accounts receivable balance for March of 2024. We reviewed AFRS journal voucher 54009801, which was prepared and uploaded on April 3, 2024 by Son Pham, Fiscal Analyst and reviewed and released by Shelly Peterson, Assistant Treasury Manager on April 3, 2024.

The explanation of the journal entry was listed as "To record fund 620 financial transaction for the month of March 2023". The total for the JV was \$32,658,822.41 and contained various entries to GLs 1110, 3210, and receivables. All entries were in fund 620, revenue source 0471 (Unemployment Compensation Contributions). The amount booked to GL 3205/1312 accounts was a decrease in employer A/R in the amount of (\$1,608,339.41) using trans code 020.

We reviewed the spreadsheet and noted a schedule of Accounts Receivable for the month ending March 2024, which showed the change in A/R GL 1312 from the previous month. It contained screen shots of reports and pivot tables identifying the March 2024 ending receivable balance of \$96,578,519.28 and the March 2024 beginning receivable balance of \$98,186,858.69. The change in A/R for March was (\$1,608,339.41) which

## State of Washington

tied to the journal voucher.

**No issues noted.**

**Noted Weaknesses are as follows:**

- None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.2.PRG - Receivables (Net of Allowance)**

*Procedure Step:* Key Control #2 NGTS (Manual)

*Prepared By:* DRR, 10/14/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

## State of Washington

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood*

## State of Washington

*of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done.:

## State of Washington

**Key Control 2 (Existence/Valuation - Manual):** The Treasury Manager or Assistant Treasury Manager reviews journal vouchers to record the incremental change to the allowance for doubtful accounts. The Treasury Manager reviews the quarterly Allowance for uncollectible accounts receivable schedule prepared by the Fiscal Analyst and the supporting query results to ensure the estimate reflected operations and historical trends.

The understanding for this system is documented above in the "Controls - NGTS" step.

### **1. Confirmation of Key Manual Control:**

We obtained journal vouchers 54099816 (to record NGTS Allowance as of 6/30/2024) and 54014807 which adjusted the NGTS allowance for doubtful accounts to calculated five-year average of uncollectible (written-off) receivables. We noted the journal vouchers were prepared by Son Pham, Fiscal Analyst, on 8/30/2024 and were approved by Meghan Phelps, Treasury Manager, on 8/30/2024.

We reviewed the journal voucher support and noted the Fiscal Analyst averaged write-offs or amounts certified as uncollectible from 2020 through 2024. The average as of 06/30/2024 was \$2,562,517.16. We also noted the workpapers, which included the 2024 NGTS Allowance Calculation spreadsheet with tabs that included both journal entries, the "option 2 write off average" tab, a detail write off report from 2020 through 2024 from NGTS, and a tab showing the effect of the Journal to AFRS on GL1342. This tab included the June 2024 beginning balance in GL1342, the amount recorded to increase the allowance for Uncollectible A/R, and the Allowance year end adjustment to bring the balance to the amount calculated on the "option 2 write off average" tab.

Additionally, we recalculated this amount without exception here [[Allowance for Doubtful Accounts Testing - NGTS](#)].

### **Noted Weaknesses are as follows:**

- The Employment Security Department used incomplete data as the basis for its certified uncollectible amount (CUA). The CUA is used to calculate the NGTS allowance. From 2018 to 2021, and in 2024 the CUA was significantly higher than in 2022 and 2023. **See issue in conclusion.**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.2.PR.G - Receivables (Net of Allowance)**



# State of Washington

*Procedure Step:* Risk Assessment  
*Prepared By:* DRR, 7/17/2024  
*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

- *General Considerations*
  - *Does the balance include transactions that are difficult to audit or involve complex accounting issues?*
  - *Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*
  - *Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*
- *Inherent Risk due to Error*
  - *How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*
  - *Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

## State of Washington

- *Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*
- *Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*
- *Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*
- *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*
  - *Are there substantial pressures or motivations to misstate the balance?*
- *Inherent Risk due to Misappropriation*
  - *Is the account balance or transaction class susceptible to sizable misappropriation?*
- *Inherent Risk due to Non-Compliance*
  - *Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*
  - *Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*
  - *Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a

## State of Washington

combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

- **Existence – SIGNIFICANT RISK**

## State of Washington

- **Valuation - SIGNIFICANT RISK**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

- **UTAB – Existence**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

- **UTAB – Valuation**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

- **NGTS – Existence**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

- **NGTS – Valuation**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

- **Existence – VERY HIGH**
- **Valuation – VERY HIGH**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following

## State of Washington

tests:

- **UTAB** Accounts Receivable - Including Fraud
  - We will select a sample of accounts receivable reported as of 6/30/2024 and review existence through subsequent payments made on repayment plans or pursuit of legal action (liens, garnishments, etc.) **(Existence)**.
- **UTAB** Accounts Receivable - Waivers
  - We will select a sample of federal waivers that were applied during FY24 and determine if they were correctly excluded from accounts receivable **(Existence)**.
- **UTAB** Allowance for Doubtful Accounts - Including Fraud
  - We will recalculate the allowance for doubtful accounts to ensure the ESD followed the correct process and determine if we agree with the methodology **(Valuation)**.
- **NGTS** Accounts Receivables
  - We will select a sample of accounts receivable from one or more of the 6/30/2024 queries that make up the accounts receivable balance. We will review existence through subsequent payments **(Existence)**.
- **NGTS** Allowance for Doubtful Accounts
  - We will recalculate the allowance for doubtful accounts to ensure the ESD followed the correct process and determine if we agree with the methodology **(Valuation)**.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### E.2.PRG - Receivables (Net of Allowance)

*Procedure Step:* Substantive Test  
*Prepared By:* DRR, 10/16/2024  
*Reviewed By:* RKM, 12/10/2024

Purpose/Conclusion.*
----------------------

# State of Washington

## **Purpose:**

To determine whether reported receivables represent amounts uncollected as of the end of the period **(Existence)**.

To determine whether receivables were reported at properly valued or calculated amounts **(Valuation)**.

## **Conclusion:**

We determined that reported receivables represent amounts uncollected as of the end of the period **(Existence)**.

We determined that receivables were reported at properly valued or calculated amounts **(Valuations)** with the following exceptions:

- (UTAB Allowance) ESD referenced the FY23 multiplying factor instead of the FY24 multiplying factor when calculating their UTAB Allowance for Doubtful Accounts and double counted the receivables related to federal waiver applications. **See issue here : [E: ESD UTAB Allowance Calculation Error]**
- (NGTS Allowance) ESD continues to use negative and low certified uncollectible amounts from prior periods when calculating their NGTS Allowance for Doubtful Accounts. **See issue here: [E: ESD Certified Uncollectible Amount].**

**See AOM here: [Aggregation of Misstatements (GAAP)].**

Testing Strategy:

The following is a list of **considerations** for testing the existence assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Receivables**

- Confirm receivables with the obligated party.
- Confirm intergovernmental receivables with the other agency.
- Confirm trade receivables using negative or positive confirmations to customers. *NOTE: if trade receivables were not confirmed, auditors should document the reasons for not following the audit requirement (see policy/criteria tab).*
- Verify receivables to source billing documents, reimbursement requests or other documentation.
- If receivables are sent to an external collection agency or trigger an action that affects the obligated party (ie: water shut-off) within a reasonably short time period, trace or reconcile from the A/R Aging report to the collection agency's report or evidence of a confirming action.
- Verify receivables through subsequent receipt of funds (remittance documentation should evidence the period to which it applies).
- For the period following balance sheet date, scan the accounts receivable general ledger control account for material charge-off and unusual transactions, and investigate.

Perform analytical procedures to determine the reasonableness of receivable balances and follow-up on any unexpected results. For example, trend analysis of aged A/R, trend of beginning balance, billings, adjustments, payments and ending balance, inventory/volume usage

## State of Washington

reconciliation, etc.

The following is a list of **considerations** for testing the valuation assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

- Review the entity's calculation of the value of intangible assets.
- Review the entity's calculation of write-off of inventory or other assets due to obsolescence or damage.

### Calculation or Realizable Value of Receivables

- Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.
- Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **SAO Audit Policy [6350](#) – External Confirmations**

Record of Work Done:

### **Substantive tests performed to meet the Existence assertion:**

UTAB Accounts Receivable Testing: [[UTAB Receivables Testing](#)]

We tested the UTAB report "Aging Receivables - Detail" for completeness against the screen shot of the UTAB report "Aging Receivables - Detail" through 6/30/2024 ran on 7/1/2024 by ESD. To ensure we could rely on UTAB's accounts receivable aging report for sample testing, we compared the "Aging Receivables - Detail" (created on 7/1/2024) with AFRS GL balances 1319 Other Receivables for fund 620 and 622 through 6/30/2024 run from Enterprise reporting.

- We removed revenue types that included pending descriptions, and excluded fraud receivables in process. After this adjustments we noted the UTAB AR total was different than the GL total by \$34,063, which is below the floor.

## State of Washington

- **We determined we could rely on the UTAB report data for testing purposes.** See tab, "Completeness UTAB Data" at: [UTAB Receivables Testing]. *No issues noted.*

### **Regular Receivables:**

Our regular receivables population consisted of over payments (by claimant) and revenue source. Due to the size of the population and the high level of detail provided by UTAB, we determined random sampling would be the most effective and efficient test. We used the TeamStore sampling spreadsheet to determine our sample size. Our sample was based on an expected misstatement rate of 0%, a tolerable misstatement rate of 7.5% and a very high assurance level. Our planned sample included 60 items. We exported the UTAB report "Aging Receivables - Detail" through 6/30/2024 and noted that we were not able to export the full population due to the size limitation of the UTAB detail reports. We downloaded a report with the "maximum number of detailed rows that could be displayed" by the system and selected from the transactions contained in it. We determined that the following revenue types made up the majority of the balance:

- 17.92% Receivable Interest Open Balance (Uncollectible Debt)
- 64.45% Receivable Principal Open Balance (Uncollectible Debt)

Our random sample pulled both the Receivable Principal and Interest Open Balance (Uncollectible Debt) types of revenue transactions from the UTAB detail report.

We reviewed the following documentation in the UTAB system to determine existence of receivables as of 06/30/2024:

- Monthly Overpayment Letters/Determination Letters sent to claimants to record the receivable amount for the month of June or July 2024.
- Repayment plans created for the claimant
- Liens filed against the claimant
- Garnishments from claimant's bank or employer
- Repayments in subsequent periods

We determined that all 60 receivables existed based on documentation in the UTAB system. **See tab, "UTAB Receivable Testing Regular" at: [UTAB Receivables Testing]. *No issues noted.***

### **Fraud Receivables:**

To obtain our fraud receivables population, we used the cube version of the UTAB Aging Receivables report, dated 7/1/2024, to export a detail report of the fraud receivables at 6/30/2024. Due to the size of the population and the high level of detail provided by UTAB, we determined random sampling would be the most effective and efficient test. We used the TeamStore sampling spreadsheet to determine our sample size. Our sample was based on an expected misstatement rate of 0%, a tolerable misstatement rate of 7.5% and a high assurance level. We used a high assurance level on the fraud receivables balance as this balance is significantly smaller than the "regular receivables" balance which was set at very high assurance needed in testing. Our planned sample included 39 items. We exported the UTAB report "Aging Receivables - Detail" through



## State of Washington

6/30/2024 and noted that we were not able to export the full population due to the size limitation of the UTAB detail reports. We downloaded a report with the "maximum number of detailed rows that could be displayed" by the system and selected from the transactions contained in it. We determined that the following revenue types made up the majority of the balance:

- 11.78% Receivable Interest Open Balance (Uncollectible Debt)
- 72.38% Receivable Principal Open Balance (Uncollectible Debt)

Our random sample pulled only the Receivable Principal and Interest Open Balance (Uncollectible Debt) types of revenue transactions from the UTAB detail report.

We reviewed the accounts for the following documentation in the UTAB system to determine existence of reported receivables as of 06/30/2024:

- Monthly Overpayment Letters/Determination Letters sent to claimants to record the receivable amount
- Repayment plans created for the claimant
- Liens filed against the claimant
- Garnishments from claimant's bank or employer- N/A
- Repayments in subsequent periods/fraud recovery

We determined that all 39 fraud receivables existed based on documentation in the UTAB system. **See tab, "UTAB Receivable Testing Fraud" at: [\[UTAB Receivables Testing\]](#). *No issues noted.***

### **NGTS Accounts Receivable Testing**

We reviewed the composition of NGTS receivables in our reconciliation at: [\[NGTS Receivables Testing\]](#). Tab, "Completeness NGTS Recon". We noted SQL Query #1 - Liable Q2 Amounts Assessed for Q2 totaled approximately \$373.6M or about 77% of the total accounts receivable balance (fund 620 GL 1312). We obtained the SQL query results from Meghan Phelps, Treasury Manager, and tied the report total to our reconciliation. Amounts tied without exception.

We noted our population included 317,756 assessments or employer accounts. We determined random sampling would be the most effective and efficient test. We used the Financial Audit Substantive Sample testing spreadsheet to determine our population based on an expected misstatement rate of 0%, 7.5% tolerable misstatement rate, and a very high assurance level. Our sample population totaled 60 assessments or employer accounts. We randomly selected the 60 samples.

We reviewed Q2 assessments in NGTS and ensured the amount tied to the query results. We determined the existence of the receivable as of June 30, 2024 by tying the amount of the assessment to the subsequent payment, collections documentation, or application of credits on account. See testing at: [\[NGTS Receivables Testing\]](#). ***No issues noted.***

Waiver Testing:

## State of Washington

We requested a population of all federal waivers applied between July 1, 2023 and June 30, 2024, which was provided as "SQR 13135 SAO EGC Waivers.xlsx" by Stephanie Eskesen, Audit Liaison. Due to the size of the population, we determined random sampling would be the most effective and efficient test. We used the TeamStore sampling spreadsheet to determine our sample size. Our sample was based on an expected misstatement rate of 0%, a tolerable misstatement rate of 7.5% and a very high assurance level. Our planned sample included 60 items. We used the claim IDs provided in our sample to look up the waivers in UTAB to ensure the waiver was correctly excluded from accounts receivable with a credit to the claimants account. See testing at: [\[Federal Waiver Testing\]](#). **No issues noted.**

### **Substantive tests performed to meet the Valuation assertion:**

#### **UTAB Accounts Receivable Testing**

We recalculated payments in UTAB at: [\[Premiums and Claims\]](#). We determined this work was sufficient to ensure UTAB was calculating overpayments correctly.

#### **NGTS Accounts Receivable Testing**

We recalculated premiums in NGTS at: [\[Premiums and Assessments\]](#). We determined this work was sufficient to ensure NGTS was calculating premiums correctly.

#### **UTAB Allowance for Doubtful Accounts**

**See testing here:** [\[Allowance for Doubtful Accounts Testing - UTAB\]](#)

##### Non Fraud Allowance:

The UTAB non-fraud allowance for doubtful accounts is based on monthly collection data by aging category and the year-end amounts. We based our recalculation steps on the Department's desk manual. We performed the following steps:

1. Determine the annual average collection history by aging category.
  - First, we obtained the "Age of Account Payments" report from UTAB for each month in the fiscal year. This report totaled collections by revenue source and aging category of the repayment plan. We recorded the total amounts receipted for each aging category for every month of fiscal year ended June 2024. We averaged the totals and determined the average amount receipted as a percent for each aging category.
2. Determine how many past-due repayment plans will likely be collected.
  - UTAB also tracked repayment plans that were not being repaid (no payments for 180 days or more). This data was reported on UTAB report "Uncollectible Balances". We multiplied the total Uncollectible Balances (less any previous aging category balances) by the respective annual average aging category percent. This determined the amount expected to be eventually collected.
3. Determine the amount of repayment plans that are likely to be written off in a dollar value and percent
  - The amount expected to be collected less the total uncollectible balance was the amount expected to be written off. The amount expected to be written off was divided by the total uncollectible balances to determine the expected write-offs or multiplying factor (percent).
4. Multiply the amount expected to be written off by total regular accounts receivable (for each fund).

## State of Washington

- Last, we multiplied the regular accounts receivable balance by fund by the multiplying factor to determine the allowance for doubtful accounts for each fund. We calculated the same multiplying factor as the Department without exception, however, when calculating their UTAB Allowance, ESD referenced the FY23 multiplying factor and not the FY24 multiplying factor in their excel calculation document. This error and ESD including federal waivers in their calculation resulted in overstatement their GL1349 for fund 620 by \$3,096,136 and overstatement in GL1349 in fund 622 by \$14,010,152. For a total overstatement of \$17,106,288 in GL1349.

We determined the calculation methodology was appropriate and based on accurate collection information or bad debts (write-offs), as the UTAB system automatically writes off receivable accounts that have been inactive (no payments made) for 180 days.

**We determined ESD has taken corrective action regarding our finding from FY23. We verified that data used in the calculation of the allowance was accurate and agreed to accounting records, however, ESD referenced the incorrect cell in their allowance calculation and included additional steps to include federal waivers in their calculation which resulted in double counting the related receivable in their allowance calculation, and should have been caught during management review. See Issue and AOM link in the conclusion above.**

See tab, "Non-Fraud Allowance" at: [[Allowance for Doubtful Accounts Testing - UTAB](#)].

### Fraud Allowance:

During FY24 the ESD also calculated an expected fraud uncollectible estimate. This was due to the fraud that occurred during FY20 in regards to the unemployment benefits. ESD worked with OFM to determine the percentage that would be the allowance for fraud receivables. They took the total UTAB receivables and determined the portion related to fraud. Once they determined that they took the fraud receivables amount and reduced it by any items still in process as of June 30, 2024. Once they had this amount they divided it by the receivables amount to determine the percentage that was determined uncollectible. We calculated 97% to be the allowance for fraud. This tied to ESD's percentage without exception. We reviewed the UTAB allowance calculation document and supporting documentation provided by Meghan Phelps, Treasury Manager, to verify that the percentage seemed reasonable for the fraud allowance for doubtful accounts. We determined that 97% is a reasonable estimate.

See tab, "Fraud Allowance" at" [[Allowance for Doubtful Accounts Testing - UTAB](#)].

### Federal Waivers

The receivable balance in GL1319 includes the receivables related to federal waiver applications and are already captured in ESD's normal allowance for doubtful accounts calculation. ESD performed additional steps to include the receivables related to the waivers in their allowance calculation, which resulted in a double counting of these receivables. This resulted in a misstatement and is included in issue 16 along with the referencing of the incorrect cell in ESD's allowance calculation. **See issue and AOM link in the conclusion above.**

### **NGTS Allowance for Doubtful Accounts**

## State of Washington

Note: We reached out to Corbin Foster, Enterprise Financial Recover Manager (aka Collections Manager), on November 27, 2024 to inquire about the ESD Collections Team's progress in catching up on their collections work related to Certified Uncollectable Account (CUA). Corbin wanted to clarify our understanding of "Collections being placed on hold during the pandemic". He mentioned that in the early days of the pandemic, agency leadership decided to pause active collections, meaning for example the filing of liens against individuals and employers, the garnishing of assets such as wages or bank accounts, and proactively contacting customers to request payment. Throughout these past several years, ESD has allowed and welcomed customers who contacted them to voluntarily remit payment or enter into long-term payment plans, and ESD has also continued offsetting benefits against any overpayment balances. The collections pause was lifted for employers in December 2023 and ESD is in the early stages of lifting the collections pause for UI claimants with benefit overpayments.

Corbin informed us that employer collections are still a work in progress. As of March 2020, there were an estimated 4.5k employers who owed a collective estimated total of \$35 million in principle, penalties & interest. This amount has grown to approximately 15k employers owing approximately \$102 million in principle, penalties, and interest as of December 3, 2024, mostly due to the pandemic. Additionally, Corbin mentioned that he expects the majority of this \$102 million to be collectible, as only about 3.5k employers are inactive (closed their business), and the remaining business are actively conducting businesses, and are generating operating revenues, which can be used to satisfy their outstanding balance owed to ESD.

We used the above information to estimate the potential NGTS receivable allowance error. **See potential error here** [[Potential NGTS Allowance Error](#)]. We estimated that the CUA based on the above information should have been approximately \$23.8 million greater than was used in the Departments calculations which resulted in an understatement of the NGTS receivable allowance by approximately \$4.76 million. Additionally, the Department should have reduced their NGTS receivable balance by the \$23.8 million as they have been aware of this information throughout the fiscal year.

ESD's NGTS allowance for doubtful accounts method is based on bad debt write-offs or balances determined certified uncollectible amounts (CUA). ESD used a five year average (fiscal year end June 2020 through 2024) to determine what the allowance for doubtful accounts should be for fiscal year 2024. This method was consistent with the NGTS allowance calculation used in prior years.

We obtained the detailed (transaction level) CUA data for fiscal year 2024. See tab "Option 2-Write Off Details" in our testing at [[Allowance for Doubtful Accounts Testing - NGTS](#)]. We noted the data was isolated to NGTS revenue streams (i.e. assessment types). We used the data to create a pivot table that summarized the amounts determined certified uncollectible and the date when written off. After we manually added the correct fiscal year the Excel pivot table automatically summarized the dates by fiscal year.

See tab "SAO NGTS CUA Summary" in our testing at [[Allowance for Doubtful Accounts Testing - NGTS](#)]. We used the summary level data to recalculate the amount of CUA's for each fiscal years ended 2020 through 2024. See tab "NGTS Allowance Testing" in our testing at [[Allowance for Doubtful Accounts Testing - NGTS](#)]. We recalculated the average CUA for fiscal year ended 2024 and used a five year average. The average tied to GL 1342 without exception. However, ESD has received audit issues in the FY22 and FY23 audits due to using certified uncollectible amounts (CUA) in their NGTS allowance calculation that are not reasonable. In FY22 we determined the amount should not be negative, and the FY23

## State of Washington

amount was unreasonably low compared to their historical average. We identified that ESD used the same negative CUA amount from FY22 and the low CUA amount from FY23 in their calculation of the FY24 NGTS allowance for doubtful accounts. Using the information we obtained we calculated a potential error. **See issue and AOM links in the conclusion above.**

### E.3.PRG - Premiums and Assessments

*Procedure Step:* Summary & Conclusion

*Prepared By:* CJM, 11/15/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

# State of Washington

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material](#)*

# State of Washington

*Balances spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria.:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done.:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

## **E.3.PR.G - Premiums and Assessments**

*Procedure Step:* Understanding of Line Item

*Prepared By:* CJM, 6/4/2024

*Reviewed By:* SHW, 7/23/2024

Purpose/Conclusion.:

# State of Washington

## **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

- Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.
- Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.
- Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.
- Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.



## State of Washington

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria:

Record of Work Done:

#### **(1) Prior Audit Exceptions:**

None

#### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

We noted the balance included activity from the following fund:

620: Unemployment Compensation Account

Fund 620 makes up the entire account balance. We do not expect to see any major changes to this line item. The transactions that are included in this line item are the premiums received from the employers. We will rely on work performed at the fund level to substantiate at the government-wide level.

Insurance Premiums at the Employment Security Department (ESD) are revenues from Unemployment Insurance (UI) taxes. Employers in the state of Washington pay for unemployment insurance through unemployment taxes; workers do not pay unemployment taxes. Unemployment tax rates are recalculated each year using a formula specified in [RCW 50.29.025](#). See permanent document at [\[FW ESD Contacts \(re SAO inquiry re RCW 50.29.025\)\]](#) for additional information related to [RCW 50.29.025](#) and the information provided by the Assistant Attorney General (AAG) over there being two RCWs within this section [(as amended by 2011 c 3) and (as amended by 2011 c 4)]. The tax rates are based on the employer

## State of Washington

payment and reporting data from the state's fiscal year even though the tax rates are in effect from January through December. The state unemployment insurance tax consists of two components, the experience-rated tax and the social-cost tax.

The employer's experience-rated tax is based on the amount of unemployment benefits paid to former employees over the past four years and the payroll size. It's determined by taking the benefit charges associated with the employer and dividing that by the total wages paid by the employer. Each employer is then assigned to one of 40 rate classes based on this number. They move up or down these classes based on their past experience.

The social-cost tax recovers costs from the previous year that can't be attributed to a specific employer. In prior years, ESD determined the flat social-cost tax by dividing the total social cost by the total taxable payroll. Based on the assigned rate class, the employer was assigned to one of twenty one social rate multipliers as specified in [RCW 50.29.025](#). However, during FY22 [Senate Bill 5873](#) made changes to the flat social tax rates assigned by [Senate Bill 5061](#) (during FY21). For rate year 2011 and thereafter, the calculation may not result in a flat social cost factor that is more than one and twenty-two one-hundredths percent except for:

- Rate year 2021 the calculation may not result in a flat social cost factor that is more than five-tenths percent (.5%)

- Rate year 2022 the calculation may not result in a flat social cost factor that is more than five-tenths percent (.5%)

- Rate year 2023 the calculation may not result in a flat social cost factor that is more than seven-tenths percent (.7%)

- Rate year 2024 the calculation may not result in a flat social cost factor that is more than eighty-five one-hundredths percent (.85%)

- Rate year 2025 the calculation may not result in a flat social cost factor that is more than nine-tenths percent (.9%)

The flat social cost is then multiplied by the assigned multiplier to determine the total social-cost tax for each employer. This social-cost tax is added to the experience-rate tax to determine the employer's total UI tax rate. There are also delinquent tax rates that are added on to the experience-rated tax and social-cost tax for employers who did not pay their total taxes the prior year.

According to ESD's Website - [Determining Your Tax Rates](#), the 2024 average total tax rate is 1.35%, a decrease from 1.43% in 2023. According to ESD's Website - [Taxable Wage Base](#), during FY24, employers will pay taxes on the first \$68,500 of each employee's wages. This increased from \$67,600 in 2023. On a quarterly basis, employers file and pay their UI taxes.

The transactions that are included in this line item are the premiums received from the employers. Insurance premiums are under fund 620 - Unemployment Compensation Account with Source 71 - Unemployment Compensation Contribution. ESD uses the Next Generation Tax System (NGTS) for calculating and collecting all premiums.

On 5/8/24, we inquired with Jeff Robinson, Labor Market Analysis/UI Research & Forecasting Manager, and Meredith Cole, Benefits Specialist 4, about significant changes. Jeff stated there have been no new changes to social-cost rate changing since FY22 due to [Senate Bill 5873](#). Jeff confirmed there were no new legislative changes that affected rates for FY24.

# State of Washington

## **(3) Updates to Significant Account Matrix:**

None

## **E.3.PR.G - Premiums and Assessments**

*Procedure Step:* Controls - NGTS

*Prepared By:* CJM, 6/28/2024

*Reviewed By:* RKM, 11/7/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

## State of Washington

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable).

## State of Washington

Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **Material Balance(s) and Assertions**

Internal controls in the NGTS address the following balance(s):

Statement of Revenues, Expenses, and Changes in Net Position - Proprietary Funds

# State of Washington

Premiums and Assessments

Statement of Activities - Government Wide

Unemployment Compensation - Charges for Services

For the following assertions:

Completeness: There is a risk that all reported revenues occurring in the fiscal period were not reported.

Valuation: There is a risk premiums and assessments are incorrectly calculated.

## **Gain an Understanding of Internal Controls**

On 5/8/2024 we met with Meredith Cole, Benefit Specialist, and Jeff Robinson, Labor Market/UI Research & Forecasting Manager, to update our understanding over premiums and assessments (assigning tax rates).

Initially new employers are assigned a North American Industry Classification system (NAICS) rate by the Labor Market and Performance Analysis (LMPA) based on the industry average for the business activity of the applicant. After two years of providing timely wage reports and payments the employer will qualify for a lower experience rate. LMPA calculates the taxable wage base used by every employer and the social flat cost rate for the year applicable to each employer's tax rate based on state law within RCWs. During FY21 [Senate Bill 5061](#) assigned the flat social tax rate of .5%. During FY22 [Senate Bill 5873](#) made changes to the flat social tax rates assigned by Senate Bill 5061. For rate year 2011 and thereafter, the calculation may not result in a flat social cost factor that is more than one and twenty-two one-hundredths percent except for:

Rate year 2021 the calculation may not result in a flat social cost factor that is more than five-tenths percent (.5%)

Rate year 2022 the calculation may not result in a flat social cost factor that is more than five-tenths percent (.5%)

Rate year 2023 the calculation may not result in a flat social cost factor that is more than seven-tenths percent (.7%)

Rate year 2024 the calculation may not result in a flat social cost factor that is more than eighty-five one-hundredths percent (.85%)

Rate year 2025 the calculation may not result in a flat social cost factor that is more than nine-tenths percent (.9%)

[Senate Bill 5873](#) also gave many small employers with 10 or fewer employees in fourth quarter 2021 more relief on their social tax rate in 2023.

Employers in rate classes 8 to 40 will get the social tax rate for rate class 7.

Employers in rate classes 1 to 7 will stay at their social tax rate.

LMPA relies on a computer generated report (ESD Referred to this report as LMPA\_AAW) to completely and accurately identify financial activity pulled to calculate the Taxable Wage Base and Social Cost tax rate. The financial activity report used in calculating the rates is produced by the Quarterly Census of Employment and Wage (QCEW) unit of the Employment Security Department (ESD). The QCEW unit collects the quarterly Unemployment Insurance tax reports from employers and then processes/verifies and edits the wage and employment records. Wage and employment information is used as the basis for calculating the average annual wage and contribution amount. To ensure accurate insurance premium revenues, the taxable wage base and the Flat Social Cost factor for the year is determined using the computer generated financial activity report or calculated in accordance with RCWs (**Key Control 1 - Valuation**).

## State of Washington

Tax rates are calculated by NGTS as specified in [RCW 50.29.025](#). NGTS calculates the Employer's experience-rated tax (component of total employer tax rate) based on the amount of unemployment benefits paid to former employees over the past four years and the payroll size. It's determined by taking the benefit charges associated with the employer and dividing that by the total wages paid by the employer. Each employer is then assigned to one of 40 rate classes based on this number. Employers are notified of their UI tax rate in December of each year. The data used for calculating UI annual tax rates are based on employers' account information as of September 30th. The UI tax rate for an employer is dependent on several factors; the employer's benefit ratio, delinquent balance, social cost rate, legislative limit, and Employer Assistant Fund. Once the rate has been calculated, the system determines the amount which should have been billed (received in payment), as the employer would have calculated the taxes owed the same as the system. Tax rates are calculated by NGTS as specified in [RCW 50.29.025](#) (**Key Control 2 - Valuation**).

### Payments

After the employer is registered and has paid employees, the employer reports employee wages and hours to ESD electronically through Employer Account Management Services (EAMS). EAMS is a program that collects the wage data that is then uploaded into NGTS for payment (not considered significant accounting systems). Paper tax & wage reports are mailed to the ESD mail room or to the retail lock box. Payments for Insurance Premiums due are submitted through e-pay or mailed to the retail Lockbox or ESD mailroom. State agencies make up the rest of the collections.

Every quarter employees must file and pay their unemployment insurance taxes using one of the following methods.

- Original paper forms that are sent to a Retail Lockbox

- A special request must be made for these paper forms

- Electronic filing through the Employer Account Management Services (EAMS)

- ePay

- Automatic Clearing House (ACH) electronic payment

Tax Calendar			
Quarter One (Q1)	January Q4 taxes due 1/31	February	March Q1 ends 3/31
Quarter Two (Q2)	April Q1 taxes due 4/30	May	June Q2 end 6/30
Quarter Three (Q3)	July Q2 taxes due 7/31	August	September Q3 end 9/30
Quarter Four (Q4)	October Q3 taxes due 10/31	November	December Q4 end 12/31

## State of Washington

The transactions that are included in this line item are the premiums received from the employers. Insurance premiums are under fund 620 - Unemployment Compensation Account with Source 71 - Unemployment Compensation Contribution. ESD uses the Next Generation Tax System (NGTS) for calculating and collecting all premiums.

### **How Transactions are Recorded in AFRS:**

#### Treasury's Reconciliation

On 5/22/24, we met with the following people to update our understanding over premiums and assessments (treasury's reconciliation):

Meredith Cole, Tax Supervisor

Janel Lamm, Tax Specialist 4

Tina Drew, Tax Specialist 4

Meghan Phelps, UI Treasury Manager

ESD performs NGTS reconciliations daily except on Tuesday when no bank statement is available. The daily NGTS reconciliation is performed by Tina Drew, Tax Specialist 4. The reconciliation starts with the NGTS report, Daily Bank Deposit Worksheet. This report itemizes the different deposit sources, payments, the amount posted by the bank, and the receipts posted in NGTS. Tina reconciles the Daily Bank Deposit Worksheet to US Bank activity (BAI2 report) **(Key Control 3 - Completeness/Valuation)**. Differences between bank deposits and NGTS are calculated and shown in a column. These differences, are due to timing differences between the bank and NGTS (i.e. payment didn't post so they have to make an adjustment to a different day). To reconcile these differences the dates of the NGTS reports are revised to reflect the bank's deposits.

Son Pham, Fiscal Analyst 4, posts the NGTS activity (from the BAI2 report) in the "Monthly AFRS JV" spreadsheet to ensure US Bank, AFRS, and NGTS activity are accurate. A bank reconciliation is then performed by My-Phuong Tran, Fiscal Analyst 3, to ensure the deposits posted by the bank agrees to the NGTS receipts and all items expected are received by the ESD. A Fiscal Analyst will review the BAI2 report on a daily basis and post to the UC Clearance Journal. At the end of the month, the Treasury Department, then uploads the total in the JV to AFRS fund 620 using the AFRS toolbox. Monthly, Meghan Phelps, UI Treasury Manager, reviews the AFRS to bank reconciliation to ensure accuracy and completeness in AFRS. She does this by comparing the Monthly AFRS JV, UC Clearance Journal and daily deposits to the total recorded in AFRS **(Key Control 4 - Completeness/Valuation)**. The ESD determines the amount of accrued revenue to recognize during their accounts receivable process and books the entry to the AR and accrued revenue as part of the monthly journal voucher, based on a SQL run by Treasury. Meghan reviews this entry as well before it is entered into AFRS **(Key Control 5 - Completeness/Valuation)**.

In 2018/2019 ESD decided to not have an interface between NGTS and AFRS for receipts. UI Treasury developed a process prior to this decision to be able to reconcile NGTS to AFRS. They use a series of SQL queries, "Agency Receipt" reports, and "BAI2" Reports".

### **Key Controls are as Follows:**



## State of Washington

**Key Control 1 (Automated)** - The taxable wage base and the Flat Social Cost factor for the year is determined using the computer generated financial activity report or calculated in accordance with RCWs, to ensure that insurance premiums and assessments are calculated correctly using these factors **(Valuation)**.

**Key Control 2 (Automated)** - Tax rates are calculated by NGTS as specified in [RCW 50.29.025](#) **(Valuation)**.

**Key Control 3 (Manual)** - A daily reconciliation is performed by a Tax Specialist to ensure the deposits posted by the bank agrees to the NGTS receipts and all items expected are received by the ESD **(Completeness/Valuation)**.

**Key Control 4 (Manual)** - Monthly, the Treasury Manager reviews the AFRS to bank reconciliation to ensure accuracy and completeness in AFRS. The Manager does this by comparing the Monthly AFRS JV, UC Clearance Journal and daily deposits to the total recorded in AFRS **(Completeness/Valuation)**.

**Key Control 5 (Manual)** - The ESD determines the amount of accrued revenue to recognize during their accounts receivable process and books the entry to the AR and accrued revenue as part of the quarterly journal voucher **(Completeness/Valuation)**.

### Noted Weaknesses are as Follows:

None

### E.3.PRG - Premiums and Assessments

*Procedure Step:* Key Control 1 (Automated)

*Prepared By:* CJM, 7/11/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion:

#### **Purpose:**

To determine whether the taxable wage base and Flat Social Cost factor for the year is determined using the computer generate financial activity report or calculated in accordance with RCWs **(Key Control 1 for NGTS)** was in place in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently

## State of Washington

during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [Controls - NGTS].

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

*g monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each*

## State of Washington

*significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live*

## State of Washington

*production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

# State of Washington

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Information Technology](#) Planning Guide**

## State of Washington

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is*

## State of Washington

*initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

## State of Washington

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined. Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.



# State of Washington

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control 1 (Automated):** The taxable wage base and the Flat Social Cost factor for the year is determined using the computer generated financial activity report or calculated in accordance with RCWs, to ensure that insurance premiums and assessments are calculated correctly using these factors (**Valuation**).

## **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - NGTS" step.

## **STEP 2: Confirm and Test Automated Key Control:**

On 5/29/24, we spoke to Jeff Robinson, Labor Market Analysis/UI Research & Forecasting Manager, to discuss the identified key control.

We identified a computer generated report (Jeff called this report the LMPA\_AAW) used by the Employment Security Department (ESD) which it relies on to completely and accurately identify the financial activity. The financial activity report is pulled by the Quarterly Census of Employment and Wages (QCEW) Unit of ESD (Jeff obtained us this report from Molly Webster, Management Analyst 5). The QCEW collects the quarterly unemployment insurance tax reports from employers and then processes/verifies the wage and employment records. This information is then used as the basis for calculating the average annual wage.

We confirmed that the data total by quarter sums in total to that used for the year within the calculations related to Key Control 1.

We verified that the query pulled the appropriate data from the database by examining the field of the source data totaled that on the report by the specific sources listed within the query. We determined this to be reasonable, because no sources outside of the query were pulled into the totals used.

Taxable Wage Base:

## State of Washington

The taxable wage base is the maximum amount of an employee total wages that is taxable under the unemployment insurance program. The maximum amount is set each year based on the average annual wage for contribution purposes (AAWCP) for the previous year. By state law, the amount of wages subject to tax for each individual shall be 115 percent of the wages subject to tax for the previous year rounded to the next lower \$100, except that the amount shall not exceed 80 percent of the "average annual wage for contributions purposes" for the second preceding calendar year rounded to the next lower \$100.

Beginning January 1, 2024, employers will pay unemployment taxes on the first \$68,500 paid to each employee. The calculation is as follows based on an Average Annual Wage in 2022 of \$85,667:

round down (115% times \$67,600) = \$77,700

This exceeds the 80% maximum

round down (80% times \$85,667) = \$68,500

See details of our recalculation on tab, "AAWCP" at: [\[Yearly Rates Recalculation\]](#). ***No issues noted.***

### Total Taxable Wage Base for the Year:

2024 - \$68,500

2023 - \$67,600

2022 - \$62,500

2021 - \$56,500

2020 - \$52,700

### Social Flat Cost Factor:

The flat social tax rate is set using [RCW 50.29.025](#).

The flat social cost factor is run for a rate year by dividing the total social cost by the total taxable payroll. The division shall be carried to the second decimal place with the remaining fraction disregarded unless it amounts to five hundredths or more, in which case the second decimal place shall be rounded to the next higher digit. The flat social cost factor shall be expressed as a percentage.

If, on the cut-off date, the balance in the unemployment compensation fund is determined by the commissioner to be an amount that will provide more than ten months of unemployment benefits, the commissioner shall calculate the flat social cost factor for the rate year immediately following the cut-off date by reducing the total social cost by the dollar amount that represents the number of months for which the balance in the unemployment compensation fund on the cut-off date will provide benefits above ten months and dividing the result by the total taxable payroll. Prior to June 30, 2021, for rate year 2011 and thereafter, the calculation may not result in a flat social cost factor that is more than one and twenty-two one-hundredths percent.

## State of Washington

During FY22, [Senate Bill 5873](#) became law and stated that for rate year 2011 and thereafter, the calculation may not result in a flat social cost factor that is more than one and twenty-two one-hundredths percent except for rate years:

- 2021 the calculation may not result in a flat social cost factor that is more than five-tenths percent (.5%)
- 2022 the calculation may not result in a flat social cost factor that is more than five-tenths percent (.5%)
- 2023 the calculation may not result in a flat social cost factor that is more than seven-tenth percent (.7%)
- 2024 the calculation may not result in a flat social cost factor that is more than eighty-five one-hundredths percent (.85%)
- 2025 the calculation may not result in a flat social cost factor that is more than nine-tenths percent (.9%)

Note: When the trust fund has at least 15 months of benefits but less than 17 months, the minimum shall be .25%.

We confirmed that the Flat Social Cost factor for the year is determined in accordance with the RCW guidelines and Senate Bill. See calculation of the Social Cost Factor on tab, "Flat Social Cost" at: [[Yearly Rates Recalculation](#)].

### **STEP 3: Understand General IT Controls**

We met with Samantha Hill, Senior Business Systems Analyst Supervisor, and Abhishek Gupta, Solutions Architect, on June 6, 2024 to gain an understanding of the general IT controls for NGTS.

ESD utilizes a Microsoft software project management platform called Azure. Azure allows for staff members of the Information Technology Services, Business Department, and Software Developers group to work together to monitor the work flow of a project. For each step of the process there is someone assigned to work on that portion of the process and leave comments and notes on the progress. ESD uses Azure to manage the software development work-flow process for NGTS. ESD ensures that no unnecessary or accidental changes are made to the NGTS system by limiting the amount of individuals that have permission to perform changes to the system. Samantha Hill mentioned that six ESD individuals act as NGTS "Owners" that have the ability to grant access for business systems analytics department, application developers, or systems administrators to the NGTS system. The NGTS owners can add people as a "members" who have the permission to edit and view items in NGTS or a "visitor" who can only view the information in NGTS. Samantha stated there were only 5 current NGTS "members". The list is monitored by ESD to ensure that no additional users have been granted permissions without prior approval from an NGTS system owner **(General IT Control 1)**.

When NGTS needs to be changed or updated a system administrator or business systems analyst will submit a change request to Information Technology Services that will initiate the request. ESD refers to change requests for NGTS as "stories" and bug fix request as "bugs", the process for both is the same. The requests are analyzed and reviewed by a Business Systems Analyst to ensure the change is necessary and possible to implement. After the review is complete the next step would be to assign a developer to the story and move it to the development stage. The assigned developer will make the requested changes to NGTS. Once the changes have been completed the story is moved to a test environment where members of a software engineer will run tests to ensure the change is functioning as expected. The tests will differ based on the complexity of the story. After the story has passed testing the next step is move it into a staging process verification process in where the story is

## State of Washington

duplicated and place it into a second testing environment where it will be tested to ensure its functioning properly by the Business Department. The Business Department will also conduct a test called the User Acceptance Test (UAT) which ensures the changes meet the end users' expectations. A Business Systems Analyst will review that the change request is completed and will move it into development to be published. A Business Systems Analyst performs a final confirmation that the change request has been completed by sending a request for verification to end users that interact with recently changed portion of NGTS to ensure the change is now functional and working as expected (**General IT Control 2**). If there were any errors or changes at this step of the work flow process they would close the story and reopen a new one to restart the process from the beginning.

### Summary of General IT Control

**General IT Control 1** - The NGTS owners can add people as a "members" who have the permission to edit and view items in NGTS, owners can also add "visitors" who can only view the information in NGTS. The permissions list is monitored by ESD to ensure that no additional users have been made without prior approval from an NGTS system owner.

**General IT Control 2** - A Business Systems Analyst will review that the change request is completed and will move it into development to be published. A Business Systems Analyst performs a final confirmation that the change request has been completed by sending a request for verification to end users that interact with recently changed portion of NGTS.

### **STEP 4: Confirm Key General IT Controls**

**General IT Control 1** - The NGTS owners can add people as a "members" who have the permission to edit and view items in NGTS or a "visitor" who can only view the information in NGTS. The list is monitored by ESD to ensure that no additional users have been made without prior approval from an NGTS system owner.

On June 6, 2024 Samantha Hill and Abhishek Gupta provided us with a walk through of the change request process with report NGTS. During the walkthrough we were able to observe the NGTS permissions process to confirm general IT control one. Samantha showed us the "People and Groups" for NGTS Owners and Members. We were able to confirm that 6 people had the permissions to add or remove members from NGTS.

The following individuals had access as a NGTS "Owners"

- Goutham Vijay Chodapuneedi, Database Specialist
- Judy Dew, Tax and Wage Systems Manager
- Samantha Hill, Sr. Business Systems Analyst Supervisor
- Tami Hummel, Sr. Business Systems Analyst
- Bruce Randell, Enterprise Software Administration Team Specialist
- Bonnie Tennyson, Office Manager

The following individuals have NGTS access as "Members"

- Michelle Belcher, Business Systems Analyst

## State of Washington

Son Le, IT Business Systems Analyst  
Mary MacLennan, Business Systems Analyst  
Robert Parris, Business Systems Analyst  
Michael Rogers, Business Systems Analyst

Based on our understanding of the general IT controls for NGTS we can confirm the NGTS permissions process matches what was described by ESD staff. No issues noted.

**General IT Control 2 - A Business Systems Analyst will review that the change request is completed and will move it into development to published. A Business Systems Analyst performs a final confirmation that the change request has been completed by sending a request for verification to end users that interact with recently changed portion of NGTS.**

On June 6, 2024 Samantha Hill, and Abhishek Gupta provided us with a walk through of the change request process within NGTS. During the walkthrough we were able to observe the Azure work flow process to confirm the general IT controls are in place. We observed the change request assigned to the work item number "191145". The request was to create a fix for an error during the process of assessment for an employer which caused that employer's information to show a canadian address. We were able to identify that the story was created on March 9th 2024 by Nathan Bode, ESD, System Administrator. On March 20, 2024 the story was reviewed and approved by Robert Parris, ESD, Business Systems Analyst. Robert moved the story to the development work flow step and assigned Jason Brewer, ESD, Application Developer, to the task on March 25, 2024. Jason completed the development process and moved the testing workflow process and stage verification on April 16, 2024. Bhanu Prakash Karumuri, Software Engineer, in the test environment completed the testing verification on May 23, 2024 and moved the story to the next workflow step. Robert Parris conducted a UAT on behalf of the business department to ensure the changes are functioning as expected. On May 28, 2024 Robert approved the story and moved to production. On June 4, 2024 Robert Parris conducted a request for verification for work item 191145 by inquiring with Cali Cook, Tax Specialist 4. Cali confirmed that the requested fix is functional and running as expected. **No issues noted.**

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **E.3.PRG - Premiums and Assessments**

*Procedure Step:* Key Control 2 (Automated)  
*Prepared By:* CJM, 7/11/2024  
*Reviewed By:* RKM, 8/6/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To determine whether tax rates are calculated by NGTS as specific in RCW 50.29.025 (**Key Control 2 for NGTS**) was in place in order to assess control risk.

**Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - NGTS\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

**STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

**Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## State of Washington

*g monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

#### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

## State of Washington

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### **Software Calculation:**



## State of Washington

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period. If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel. If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

### **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### **Manual vs. Automated Interfaces**

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules,

## State of Washington

such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors,

## State of Washington

rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The

## State of Washington

reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control 2 (Automated):** Tax rates are calculated by NGTS as specified in [RCW 50.29.025 \(Valuation\)](#).

### **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - NGTS" step.

### **STEP 2: Confirm and Test Automated Key Control:**

We reviewed the NGTS screens and re-performed the calculations for the employer below:

Pacific Air Systems, ESD Number 000-720231-00-1

First, we reviewed the Experience Rating & Benefit Charging - Tax Rates tab. The screen showed the 2024 tax rate. The Total Employer Tax Rate was set at .27, based on various factors (social cost and EAF). See below for the various factors:

Total UI Tax Rate: .93  
UI Tax Rate: .54  
Social Cost: .36

## State of Washington

EAF (Employment Administrative Fund): .03  
Rate Method: RATE-CLASS-06

Note: Tax rates are based on the calendar year.

We then reviewed the Employer Tax Account Quarter History - Q1/2024 Tax and Wages Quarter Summary/Details - Taxable Screen, which provided the following information:

Total Employer Tax Rate:  
Processed Date: 4/25/24  
Report Received Date: 4/23/23  
Report Type: Tax/Wage  
Report Source: EAMS Bilk Filing  
Gross Wages: \$2,437,031.17  
Excess Wages: \$17,498.75  
Taxable Wages: \$2,419,532.42  
UI Tax Amount: \$21,775.80  
EAF Amount: \$725.86  
Total Amount: \$22,501.66

Auditor's Recalculation:  
 $\$2,419,532.42 \times .0093 \text{ tax rate} = \$22,501.66$

There were no exceptions in the recalculation. We have determined that NGTS calculated the employer's total tax due and tax rate accurately. *No issues noted.*

### **STEP 3: Understand General IT Controls**

See our documentation of General IT Controls here [\[Key Control 1 \(Automated\)\]](#)

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **E.3.PRG - Premiums and Assessments**

*Procedure Step:* Key Control 3 (Manual)

# State of Washington

*Prepared By:* CJM, 6/28/2024

*Reviewed By:* RKM, 7/5/2024

## Purpose/Conclusion:

### **Purpose:**

To confirm a daily reconciliation is preformed to ensure that the deposits posted by the bank agrees to the NGTS receipts and all items expected are received by the ESD (**Key Control 3 for NGTS**) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

**tep 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

## State of Washington

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*



## State of Washington

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if con*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 3 (Manual):** A daily reconciliation is performed by a Tax Specialist to ensure the deposits posted by the bank agrees to the NGTS receipts and all items expected are received by the ESD (**Completeness/Valuation**).

The understanding for this system is documented above in the "Controls - NGTS" step.

### **1. Confirmation of Key Manual Control:**

On 5/22/24, we met with Tina Drew, Tax Specialist 4, and Meredith Cole, Benefit Specialist 4, to discuss the reconciliation.

To perform the reconciliation between NGTS and the bank, Tina pulled the Daily Bank Deposit Worksheet into her work queue. After she has reconciled all the items, she clicks the <approve> button which will complete her process and remove the item from her queue.

During our review, we noticed that she verifies that the total bank deposit amount agrees between the Daily Bank Deposit Worksheet and the bank statement. This verification is important as it will confirm that the bank's total deposit for the day is complete and accurate in NGTS.

## State of Washington

We selected the date of 3/11/2024 to: (1) determine whether the reconciliation was completed (that is no variance between NGTS and US bank) and (2) verify total deposit on Daily Bank Deposit Worksheet agrees to bank statement and agrees to NGTS. The amount reported on the Daily Bank Deposit Worksheet was \$620,825.38. The amount on the Bank Statement Report was reported as \$611,078.40. The amount of ACH dishonored (returned ACH transaction) was \$9,746.98. The variance between the Daily Deposit Worksheet and the US Bank statement was due to US Bank returning checks and not having the ACH dishonored amount in it's statement. The ACH dishonored amount equals the variance between the Daily Bank Deposit Worksheet and the Key Bank statement. We determined this to be reasonable since the ACH dishonored checks were a credit. ***No issues noted.***

### **Noted Weaknesses are as follows:**

"None"

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.3.PRG - Premiums and Assessments**

*Procedure Step:* Key Control 4 (Manual)

*Prepared By:* CJM, 10/2/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion.
---------------------

#### **Purpose:**

To confirm a monthly reconciliation is preformed between the bank and AFRS (**Key Control 4 for NGTS**) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## State of Washington

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important*

## State of Washington

*enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

*A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if con*

Guidance/Criteria.†

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control 4 (Manual):** Monthly, the Treasury Manager reviews the AFRS to bank reconciliation to ensure accuracy and completeness in AFRS. The Manager does this by comparing the Monthly AFRS JV, UC Clearance Journal and daily deposits to the total recorded in AFRS **(Completeness/Valuation)**.

The understanding for this system is documented above in the "Controls - NGTS" step.

### **1. Confirmation of Key Manual Control:**

On June 27, 2024, Meghan Phelps, Treasury Manager, provided us with the March 2024 Monthly AFRS JV and Tina Drew, Tax Specialist 4, provided us with the BAI2 report for March 11, 2024. The Clearance tab of the March 2024 Monthly AFRS JV records the daily amounts for transactions and totals them for the month. For March 11, 2024 there was a total of \$611,078.40 received and \$9,746.98 in ACH debts. The amounts in the clearance tab agreed to the amounts declared on the March 11, 2024 BIA2 report. We were able to determine the monthly totals in the Clearance tab tie directly to the amounts recorded in the March 2024 AFRS JV and bank. **No issues noted.**

We confirmed the Treasury Manager's review of bank statements in our control confirmations for Cash and Cash Equivalents here [[Key Control 1 \(Cash Reconciliations\)](#)].

### **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

# State of Washington

## E.3.PRG - Premiums and Assessments

*Procedure Step:* Key Control 5 (Manual)

*Prepared By:* CJM, 7/22/2024

*Reviewed By:* RKM, 8/6/2024

Purpose/Conclusion:

**Purpose:**

To confirm ESD accurately records accrued revenue to recognize during their accounts receivable process and books the entry to the AR and accrued revenue as part of the quarterly journal voucher (Key Control 5 for NGTS) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

## State of Washington

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence*

## State of Washington

*about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if con*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 5 (Manual):** The ESD determines the amount of accrued revenue to recognize during their accounts receivable process and books the entry to the AR and Accrued revenue as part of the quarterly journal voucher (**Completeness/Valuation**).

The understanding for this system is documented above in the "Controls - NGTS" step.

### **1. Confirmation of Key Manual Control:**

On 7/16/2024, we obtained the information on how journal vouchers are prepared and reviewed before being uploaded into AFRS, from Meghan Phelps, Treasury Manager and Son Pham, Fiscal Analyst.

### **Accrued Revenue**

Son showed us the "Monthly AFRS JV" spreadsheet that they use as support for recording the monthly journal entry for the month ending March



## State of Washington

2024. There are tables showing the following:

Schedule of Accounts Receivable which calculates the amount of receivables accrued for the month.

The Allowance for Uncollectible Accounts for the quarter, which shows how much allowance for uncollectible accounts should be accumulated as of the quarter ending 3/31/2024.

The amounts determined for the Accounts Receivable and Allowance for Uncollectible Accounts entry ultimately result in a change in the Accrued revenues for the period.

We verified that the amount listed on the March 2024 UC Clearance Journal matched the amounts reported on the JV. Son Pham, Fiscal Analyst, reconciles the total month's cash receipts to the Clearance Account.

The JV totals were traced to the UC Clearance Journal. No exceptions were noted.

We agreed the amount of \$32,658,822.41 in the journal voucher to the spreadsheet provided. *No issues noted.*

### **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.3.PRG - Premiums and Assessments**

*Procedure Step:* Risk Assessment

*Prepared By:* CJM, 10/2/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion:
---------------------

# State of Washington

## **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

#### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

#### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

#### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

#### *Inherent Risk due to Misappropriation*

## State of Washington

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

# State of Washington

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

## **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation - **High**

Completeness - **High**

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**NGTS** - Valuation

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## State of Washington

### **NGTS - Completeness**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation - **HIGH**

Completeness - **HIGH**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

#### **Completeness:**

We will select a sample of deposits and ensure they are complete by tracing the deposits to reconciliations and NGTS.

We will review the year-end bank statement reconciliation through our testing of the cash and cash equivalents balance.

#### **Valuation:**

We will review the employer wage reports (in NGTS) for two samples of employers (delinquent and non-delinquent) and recalculate the tax rate and premiums due for those employers. Additionally, we will review the amount estimated for accrued revenues through our testing of our account receivable balance.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **E.3.PR.G - Premiums and Assessments**

*Procedure Step:* Substantive Test

*Prepared By:* CJM, 10/22/2024

*Reviewed By:* RKM, 10/28/2024

# State of Washington

## Purpose/Conclusion:

### **Purpose:**

To determine whether all revenues relating to the period were reported (**Completeness**).

To determine whether revenues were reported at properly valued or calculated amounts (**Valuation**).

### **Conclusion:**

During our completeness testing we identified an issue related to the NGTS deposit testing. See issue here: [[E: ESD Misstatement of NGTS Deposits Reporting to AFRS](#)]. See AOM here: [[Aggregation of Misstatements \(GAAP\)](#)].

We determined revenues were reported at properly valued or calculated amounts. *No issues noted.*

## Testing Strategy:

### **Valuation**

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Calculation**

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

### **Realizable Value**

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### **Estimation / Recognition**

Review calculation and support for assumptions of any estimated revenues.

## State of Washington

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

### **Property Tax Revenues** - see separate step

The following is a list of **considerations** for testing the completeness assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Identify expected revenue streams based on understanding of fund activities and scan to see if revenue is reported for all such streams. Follow up on any unexpectedly missing streams.

Identify new revenues (ex: new grants or programs) and follow up to verify that expected revenues have been reported.

Perform a multi-year trend of revenues and follow up on unexpected decreases.

Compare revenues to budgeted amounts and follow up on unexpectedly low actual amounts.

Search for manual journal entries that debit (decrease) revenues. Consider testing if any risk indicators are noted.

### **Cut-Off**

Scan revenue transactions recorded 1-3 months before and/or after fiscal year end. Based on the scan, test selected or sampled revenues to determine if they were reported in the correct period.

### **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

Guidance/Criteria.†

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.6.11](#) Suspense Funds**

# State of Washington

Record of Work Done:

## **Substantive tests performed to meet the Completeness assertion:**

We used the Nonstatistical Sample of Population 365 or less spreadsheet with a tolerable misstatement and assurance levels dictated by the material balance workpaper for a planned sample size of 24. We randomly selected a sample of 24 business days throughout FY24, excluding days that fell on a weekend or a state/federal holiday.

We obtained Daily Bank Deposit Worksheet Reconciliations (from NGTS) and Key Bank Statement screenshots to ensure that bank deposits (revenue) are complete. We ensured that the bank deposits coming through US Bank agreed to amounts reported within NGTS.

See substantive testing at: [\[FS Sampling - NGTS Deposits Testing\]](#). Based on our evaluation of results and sampling risk, we determined the sample provided a reasonable basis for conclusions about the population. We determined there to be a known misstatement of \$122,737.33 and a total misstatement of \$1,635,945. On October 10, 2024, we inquired with Stephanie Eskesen, External Audit Liaison, and she stated that NGTS had double posted a bank deposits when the bank had only received one deposit. **See issue here** [\[E: ESD\\_Misstatement of NGTS Deposits Reporting to AFRS\]](#)

We also reviewed the year-end bank reconciliation through our testing of the cash and cash equivalents balance. See record of work done at: [\[Substantive Test\]](#).

## **Substantive tests performed to meet the Valuation assertion:**

We performed the following procedures to determine whether revenues were reported at properly valued or calculated amounts:

### Delinquent Employers Testing:

We used the Financial Audit Substantive Statistical Sample spreadsheet with a tolerable misstatement and assurance levels dictated by the material balance workpaper for a planned sample size of 39. We decided to expand the testing by 17 additional samples due to the risk associated with premiums and assessments. We randomly selected a sample of 56 delinquent employers. We reviewed the employer tax rate transaction to determine whether revenue transactions were correctly calculated. We recalculated the employers UI tax rate in effect for the 2024 Fiscal Year. The employer had two UI tax rates in effect for the year. One for the period of July 1, 2023 through December 31, 2023 and a second for the period of January 1, 2024 to June 30, 2024. This is due to tax rates being assigned based on calendar year.

The Employer's UI Tax rates are automatically calculated by NGTS and employers are notified of their rates in December of each year. The UI tax rate for an employer is dependent on several factors:

- Employer's Benefit Ratio
- Delinquent Balance
- Social Cost Rate



# State of Washington

Legislative Limit  
Employment Administration Fund (EAF) Tax Rate

During testing, we determined the following factors of the Employers UI rate through verification or recalculation based on NGTS:

Employer's Benefit Ratio (Experience Rating)

Amount of unemployment benefits paid to former employees over the past 4 years and payroll size. It's determined by taking the benefit charges associated with the employer and dividing that by the total wages paid by the employer. Each employer is then assigned to one of 40 rate classes based on this number.

Social Cost Rate

Delinquent Balance

EAF Tax Rate

Using the data obtained at [\[Population Methodology\]](#), we were able to recalculate the recorded amount of charges. For delinquent employers we used the formula of Taxable Wages \* Total Tax Rate to recalculate premiums. We compared this recalculation to another recalculation of premiums from within NGTS where we verified that tax rates and the amounts of payments were correct. See substantive testing performed at: [\[FS Sampling - Premiums & Assessments Testing\]](#). Tabs, "Delinquent NGTS Testing" and "Delinquent Testing Detail". ***No issues noted.***

## Non-Delinquent Employers Testing:

We used the Financial Audit Substantive Statistical Sample spreadsheet with a tolerable misstatement and assurance levels dictated by the material balance workpaper for a planned sample size of 39. We decided to expand the testing by 18 additional samples due to the risk associated with premiums and assessments. We randomly selected a sample of 57 non-delinquent employers. We reviewed the employer tax rate transaction to determine whether revenue transactions were correctly calculated. We recalculated the employers UI tax rate in effect for the 2024 Fiscal Year. The employer had two UI tax rates in effect for the year. One for the period of July 1, 2023 through December 31, 2023 and a second for the period of January 1, 2024 to June 30, 2024. This is due to the tax rates being assigned based on the calendar year.

Tax rates are calculated every calendar year. The Employers UI Tax rates are automatically calculated by NGTS and employers are notified of their rates in December of each year. The UI tax rate for an employer is dependent on several factors:

Employer's Benefit Ratio

Delinquent Balance

Social Cost Rate

Legislative Limit

EAF Tax Rate

During testing, we determined the following factors of the Employers UI rate through verification or recalculation based on NGTS:

Employer's Benefit Ratio (Experience Rating)

## State of Washington

Amount of unemployment benefits paid to former employees over the past 4 years and payroll size. It's determined by taking the benefit charges associated with the employer and dividing that by the total wages paid by the employer. Each employer is then assigned to one of 40 rate classes based on this number.

Social Cost Rate

Delinquent Balance

EAF Tax Rate

Using the data obtained at [[Population Methodology](#)], we were able to recalculate the recorded amount of charges. For non-delinquent employers we used the formula of Taxable Wages \* Total Tax Rate to recalculate premiums. We compared this to a recalculation of premiums from within NGTS where we verified that tax rates and the amounts of payments were correct. See substantive testing performed at: [[FS Sampling - Premiums & Assessments Testing](#)]. Tabs, "Non-Delinquent NGTS Testing" and "Non-Delinquent Testing Detail". ***No issues noted.***

### Accrued Revenue:

We reviewed the amount estimated for accrued revenues through our testing of the accounts receivable (net of allowance) balance. See record of work done at: [[Substantive Test](#)].

Note: Penalties and Interest are reported under Miscellaneous Revenue and are not part of this line item.

### E.3.PRG - Premiums and Assessments

*Procedure Step:* Population Methodology

*Prepared By:* PS, 8/27/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To created a population of delinquent taxable employers and a population of non-delinquent taxable employers.

### **Conclusion:**

We have provided the delinquent and non-delinquent taxable employers populations to the audit team.

# State of Washington

Testing Strategy:

Guidance/Criteria:

Record of Work Done:

## **Import NGTS Data**

IT Audit emailed Stephanie Eskesen, ESD External Audit Liaison, and Sam Havens, ESD Data Architecture, Transformation and Analytics Manager, to request for NGTS data. This included the NGTS wage report data, NGTS tax report data, tax rate data, and employer data.

An email was sent on May 1st, 2024, to request for the fiscal year 2024 datasets. ESD provided the fiscal year 2024 NGTS datasets text format to us on August 21st, 2024. The files were sent to SAO via the WaTech managed file transfer site (mft.wa.gov). Files were saved to the SAO network drive and imported into SQL database. We have confirmed the record count of each file received to the record count provided by ESD staff. No exception. We performed procedures at [Reasonableness NGTS 2024](#) and determined that the data are reasonable.

## **Document Test Objective and Methodology**

Team FA submitted helpdesk 68025 to request for a population of delinquent employers and a population of non-delinquent employers.

The following describes the steps taken to meet the test objective:

- Create a table of delinquent employers from the Tax Rate file, those with DelinquentTaxRate field of greater than zero.
- Create a table of non-delinquent employers from the Tax Rate file, those with DelinquentTaxRate field equal to zero.
- Add details to delinquent and non-delinquent employers by joining to the NGTS wage table or tax rate table.
- Create a summary table of delinquent employers from the detail table.
- Create a summary table of non-delinquent employers from the detail table.

As we perform our testing, we will make adjustments to this plan as necessary.

## **Queries**

The queries written to complete the testing can be seen at [Testings NGTS 2024](#).

# State of Washington

## **Reasonableness**

The reasonableness of test results has been performed and documented in the above queries. Based upon our checks, we consider our test results to be complete and reasonable.

## **Results**

Test results were provided to Team FA, through an Excel spreadsheet titled, *!2024\_Tax\_Rates\_Populations.xlsx*. The results provided contain CONFIDENTIAL DATA.

A population of FY2024 delinquent employers, with details.	42339records
A population of FY2024 delinquent employers, summary.	21324 records
A population of FY2024 non-delinquent employers, with details.	339915 records
A population of FY2024 non-delinquent employers, summary.	176334 records

## **E.3.PRG - Premiums and Assessments**

*Procedure Step:* Permanent File  
*Prepared By:* CJM, 10/29/2024  
*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion.:

### **Purpose/Conclusion:**

To document relevant information obtained during our audit which can be applicable to future audits.

Testing Strategy.:

### **Purpose/Conclusion:**

To document relevant information obtained during our audit which can be applicable to future audits.

Guidance/Criteria.:

# State of Washington

## Record of Work Done:

### **Perpetual Note**

As it relates to the contribution rates determined by ESD, we noted that [RCW 50.29.025](#), prescribes the procedures of the department in calculating their Contribution Rates. We noted there were two separate sections of the same RCW as legislature had enacted two acts amending the same section during the same year. As such, we inquired of our Assistant Attorney General (AAG) to determine the appropriate RCW which the Department should be following.

Per our inquiry, we are documenting the conclusion which the Department should be following [RCW 50.29.025](#) (as amended by 2011 c 4).

We have included the correspondence as support within the attached email at: [\[FW ESD Contacts \(re SAO inquiry re RCW 50.29.025\)\]](#), documenting this conclusion and our understanding.

### **E.4.PRG - Premiums and Claims**

*Procedure Step:* Summary & Conclusion

*Prepared By:* DRR, 9/24/2024

*Reviewed By:* CJG, 11/21/2024

## Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

## Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

# State of Washington

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

1. Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

## Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and "what could go wrong" from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?

## State of Washington

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do **not** indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **E.4.PR.G - Premiums and Claims**

# State of Washington

*Procedure Step:* Understanding of Line Item  
*Prepared By:* DRR, 5/21/2024  
*Reviewed By:* SHW, 7/31/2024

Purpose/Conclusion:

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

## **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

## **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed



## State of Washington

significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

No prior audit exceptions were noted for this line item.

#### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

We noted the balance included activity from the following funds:

620: Unemployment Compensation Account

622: Unemployment Compensation Federal Employees' Benefit Payment Account

We evaluated the funds and determined transactions from fund 620 make up most of the account balance. We noted the following significant

## State of Washington

changes to the line item:

- Fund 622 GL6505 decreased by \$118 million or 121.5%
- Fund 622 GL6510 decreased by \$1.3 billion or 98.5%
- Fund 620 GL6505 decreased by \$51 million or 101.3%
- Fund 620 GL6510 increased by \$162 million or 15.8%

The Premiums & Claims line item is composed of the payments made by warrant and direct deposit to recipients of unemployment insurance benefits. We expect this balance to agree with the Unemployment Compensation Benefit expenditures issued by the Unemployment Tax and Benefits (UTAB) platform and recorded in AFRS. Unemployment payments include unemployment for all eligible recipients.

The primary control systems covering the relevant assertions is UTAB. Activities performed by UTAB include:

- Interfacing with NGTS
- Making an initial determination of eligibility
- Calculating benefit amounts
- Issuing payments to claimants

UI benefit payments are made out of the trust fund. See below for the benefit types:

Regular Unemployment Compensation (State and Federal: UCFE, and UCX)

Weekly Benefit Amount (WBA): Dependent on state law.

Duration: 26 weeks maximum, or until the claimant reaches the end of the benefit year.

This program is for claimants that are out of work due to no fault of their own.

Pandemic Emergency Unemployment Compensation (PEUC)

WBA: Based on regular unemployment compensation.

Duration: 13 weeks.

PEUC was a federal program created in response to the COVID-19 pandemic. It provided additional benefits through Sept. 4, 2021, to workers who:

Exhausted their regular UI claim with a benefit year that ended on or after the week ending July 6, 2019.

Have left work through no fault of their own.

Are able to work, available for work, and actively seeking work as directed.

Extended Benefits (EB)

WBA: Based on regular unemployment compensation.

Duration: On December 13, 2021, federal law reduced the number of EB benefits from 20 to 13 weeks.

This program was triggered by a high unemployment rate in Washington. Claimants can get Extended Benefits only after their regular unemployment benefits and other extensions, like PEUC, have run out.

## State of Washington

Due to the lower unemployment rate in Washington state, the U.S. Department of Labor has notified ESD that Washington's Extended Benefits program was ended on March 13, 2021.

### Pandemic Unemployment Assistance (PUA)

WBA: Calculated by state accordance in Unemployment Insurance Program Letter (UIPL) No. 16-20

Duration: February 2, 2020 to September 4, 2021 (up to 39 weeks)

PUA is a benefit program that provides a financial safety net to many people who do not qualify for regular unemployment, including:

- Self-employed people

- Independent contractors

- Part-time workers (with fewer than 680 hours)

To be eligible for this program the claimant must have a COVID-19 related reason.

### Federal Pandemic Unemployment Compensation (FPUC)

WBA:

- \$600 (until July 25, 2020)

- \$300 (until September 4, 2021)

Duration:

- \$600: March 29, 2020 to July 25, 2020

- \$300: January 2, 2021 to September 4, 2021

FPUC was an additional amount that was added to the claimant's weekly benefit.

### Lost Wages Assistance (LWA)

WBA: \$300

Duration: Weeks ending August 1, 2020 to September 5, 2020

ESD was approved for the LWA program through the Federal Emergency Management Agency (FEMA). LWA was a federal program that added \$300 for each week the program was federally funded. If the claimant received unemployment benefits for the approved weeks and they were unemployed or working fewer hours due to disruption by COVID-19, then they were eligible for the benefits.

### Pandemic Relief Payments (PRP)

Amount: \$550

Duration: One-time payment for week ending November 21, 2020

On December 27, 2020, Governor Jay Inslee authorized the use of federal CARES Act funds to help Washington claimants whose PUA benefits expired on December 26, 2020 and were waiting for federal legislation to extend those benefits. Federal legislation was signed into law on December 27, 2020 which extended, expanded, and changed the CARES Act provisions. Regardless, claimants eligible for the one-time Pandemic Relief Payment still received it.

### Shared Work

## State of Washington

WBA: \$201 - \$844

Duration: 1 year

Shared Work allows the employer to reduce a claimant's hours by as much as 50 percent, while the claimant collects benefits to replace a portion of their lost wages.

### Trade Readjustment Allowances (TRA)

WBA:

Dependent on petition number.

Duration:

Dependent on petition number.

This program assists workers who have become unemployed as a result of increased imports from, or shifts in production to, foreign countries. The goal of the Trade Act programs is to help trade-affected workers return to suitable employment as quickly as possible.

### Reemployment Trade Adjustment Assistance (RTAA)

WBA:

Dependent on petition number.

Duration:

Dependent on petition number.

This program assists workers who have become unemployed as a result of increased imports from, or shifts in production to, foreign countries. The goal of the Trade Act programs is to help trade-affected workers return to suitable employment as quickly as possible.

### Disaster Unemployment Assistance (DUA)

WBA: Dependent on gross wages. It is calculated using the same formula as regular UI.

Duration: January 5, 2022 - July 9, 2022

DUA provides temporary benefits to people who lost or experienced interruptions in employment or self-employment as a direct result of a major disaster and don't qualify for regular UI. There was a declaration of a major disaster on January 5, 2022.

### Mixed Earners Unemployment Compensation (MEUC)

WBA: Extra \$100 a week for eligible programs

Duration: December 27, 2020 - September 4, 2021

ESD is implementing MEUC retroactively. Claimants are considered a mixed earner if they are using both self-employment and employment to apply for unemployment benefits.

Note: Several programs have ended, however we left information for the programs due to the Department still paying out benefits retroactively.

# State of Washington

**(3) Updates to Significant Account Matrix:**

None

**E.4.PRG - Premiums and Claims**

*Procedure Step:* Understanding of Line Item

*Prepared By:* DRR, 5/21/2024

*Reviewed By:* SHW, 7/31/2024

Purpose/Conclusion:

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

## State of Washington

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria:

Record of Work Done:

# State of Washington

## **(1) Prior Audit Exceptions:**

No prior audit exceptions were noted for this line item.

## **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

We noted the balance included activity from the following funds:

- 620: Unemployment Compensation Account

- 622: Unemployment Compensation Federal Employees' Benefit Payment Account

We evaluated the funds and determined transactions from fund 620 make up most of the account balance. We noted the following significant changes to the line item:

- Fund 622 GL6505 decreased by \$118 million or 121.5%

- Fund 622 GL6510 decreased by \$1.3 billion or 98.5%

- Fund 620 GL6505 decreased by \$51 million or 101.3%

- Fund 620 GL6510 increased by \$162 million or 15.8%

The Premiums & Claims line item is composed of the payments made by warrant and direct deposit to recipients of unemployment insurance benefits. We expect this balance to agree with the Unemployment Compensation Benefit expenditures issued by the Unemployment Tax and Benefits (UTAB) platform and recorded in AFRS. Unemployment payments include unemployment for all eligible recipients.

The primary control systems covering the relevant assertions is UTAB. Activities performed by UTAB include:

- Interfacing with NGTS

- Making an initial determination of eligibility

- Calculating benefit amounts

- Issuing payments to claimants

UI benefit payments are made out of the trust fund. See below for the benefit types:

- Regular Unemployment Compensation (State and Federal: UCFE, and UCX)

  - Weekly Benefit Amount (WBA): Dependent on state law.

  - Duration: 26 weeks maximum, or until the claimant reaches the end of the benefit year.

  - This program is for claimants that are out of work due to no fault of their own.

- Pandemic Emergency Unemployment Compensation (PEUC)

  - WBA: Based on regular unemployment compensation.

  - Duration: 13 weeks.

## State of Washington

PEUC was a federal program created in response to the COVID-19 pandemic. It provided additional benefits through Sept. 4, 2021, to workers who:

- Exhausted their regular UI claim with a benefit year that ended on or after the week ending July 6, 2019.
- Have left work through no fault of their own.
- Are able to work, available for work, and actively seeking work as directed.

### Extended Benefits (EB)

WBA: Based on regular unemployment compensation.

Duration: On December 13, 2021, federal law reduced the number of EB benefits from 20 to 13 weeks.

This program was triggered by a high unemployment rate in Washington. Claimants can get Extended Benefits only after their regular unemployment benefits and other extensions, like PEUC, have run out.

Due to the lower unemployment rate in Washington state, the U.S. Department of Labor has notified ESD that Washington's Extended Benefits program was ended on March 13, 2021.

### Pandemic Unemployment Assistance (PUA)

WBA: Calculated by state accordance in Unemployment Insurance Program Letter (UIPL) No. 16-20

Duration: February 2, 2020 to September 4, 2021 (up to 39 weeks)

PUA is a benefit program that provides a financial safety net to many people who do not qualify for regular unemployment, including:

- Self-employed people
- Independent contractors
- Part-time workers (with fewer than 680 hours)

To be eligible for this program the claimant must have a COVID-19 related reason.

### Federal Pandemic Unemployment Compensation (FPUC)

WBA:

\$600 (until July 25, 2020)

\$300 (until September 4, 2021)

Duration:

\$600: March 29, 2020 to July 25, 2020

\$300: January 2, 2021 to September 4, 2021

FPUC was an additional amount that was added to the claimant's weekly benefit.

### Lost Wages Assistance (LWA)

WBA: \$300

Duration: Weeks ending August 1, 2020 to September 5, 2020

ESD was approved for the LWA program through the Federal Emergency Management Agency (FEMA). LWA was a federal program that added \$300 for each week the program was federally funded. If the claimant received



## State of Washington

unemployment benefits for the approved weeks and they were unemployed or working fewer hours due to disruption by COVID-19, then they were eligible for the benefits.

### Pandemic Relief Payments (PRP)

Amount: \$550

Duration: One-time payment for week ending November 21, 2020

On December 27, 2020, Governor Jay Inslee authorized the use of federal CARES Act funds to help Washington claimants whose PUA benefits expired on December 26, 2020 and were waiting for federal legislation to extend those benefits. Federal legislation was signed into law on December 27, 2020 which extended, expanded, and changed the CARES Act provisions. Regardless, claimants eligible for the one-time Pandemic Relief Payment still received it.

### Shared Work

WBA: \$201 - \$844

Duration: 1 year

Shared Work allows the employer to reduce a claimant's hours by as much as 50 percent, while the claimant collects benefits to replace a portion of their lost wages.

### Trade Readjustment Allowances (TRA)

WBA:

Dependent on petition number.

Duration:

Dependent on petition number.

This program assists workers who have become unemployed as a result of increased imports from, or shifts in production to, foreign countries. The goal of the Trade Act programs is to help trade-affected workers return to suitable employment as quickly as possible.

### Reemployment Trade Adjustment Assistance (RTAA)

WBA:

Dependent on petition number.

Duration:

Dependent on petition number.

This program assists workers who have become unemployed as a result of increased imports from, or shifts in production to, foreign countries. The goal of the Trade Act programs is to help trade-affected workers return to suitable employment as quickly as possible.

### Disaster Unemployment Assistance (DUA)

WBA: Dependent on gross wages. It is calculated using the same formula as regular UI.

Duration: January 5, 2022 - July 9, 2022

## State of Washington

DUA provides temporary benefits to people who lost or experienced interruptions in employment or self-employment as a direct result of a major disaster and don't qualify for regular UI. There was a declaration of a major disaster on January 5, 2022.

Mixed Earners Unemployment Compensation (MEUC)

WBA: Extra \$100 a week for eligible programs

Duration: December 27, 2020 - September 4, 2021

ESD is implementing MEUC retroactively. Claimants are considered a mixed earner if they are using both self-employment and employment to apply for unemployment benefits.

Note: Several programs have ended, however we left information for the programs due to the Department still paying out benefits retroactively.

### **(3) Updates to Significant Account Matrix:**

None

### **E.4.PRG - Premiums and Claims**

*Procedure Step:* Key Control 1 (System Calculation - Automated)

*Prepared By:* DRR, 6/14/2024

*Reviewed By:* SHW, 8/22/2024

Purpose/Conclusion.

#### **Purpose:**

To determine whether the UTAB system determines if claimants meet the hourly eligibility requirements (at least 680 hours) to receive UI benefits **(Key Control #1 for UTAB system)** was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

# State of Washington

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

## State of Washington

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

## State of Washington

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

## State of Washington

What transactions, data, tasks, or documents are approved?  
Who are the preparers? How do preparers submit for approval?  
Who are the authorized approvers? Are there backup approvers?  
What documents or information are required to make approval judgment?  
What is the next step once a transaction/data/ task/document is approved or denied?  
Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

## State of Washington

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each*

## State of Washington

*significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is*



## State of Washington

*controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

## State of Washington

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change*

## State of Washington

*management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in*

## State of Washington

*place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

## State of Washington

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

#### **Automated Interfaces:**

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

## State of Washington

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.

If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

## State of Washington

Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.

If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

# State of Washington

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: "**This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited**".

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

## **Manual vs. Automated Interfaces**



## State of Washington

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered “manual” since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient’s age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient’s name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

# State of Washington

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

## State of Washington

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

### **Premiums and Claims - Rights & Obligations**

**Key Control 1 (Rights & Obligations - Automated):** The UTAB system determines if claimants meet the hourly eligibility requirements (at least 680 hours) to receive UI benefits.

The understanding for this system is documented above in the "Controls - UTAB" step.

### **STEP 1: Understand Automated Key Control**

The understanding for this automated key control is documented above in the "Controls -UTAB" step.

# State of Washington

## **STEP 2: Confirm and Test Automated Key Control:**

The initial eligibility requirement for unemployment insurance (UI) benefits is that claimants must have worked at least 680 hours in their base year. A claimant can file for UI benefits through an agent, online, or by using an automated phone system. UTAB determines if the claimant is eligible or not based on hours and wage data in the system. NGTS is the system of record for wage and hours data, submitted by employers.

On 5/23/2024, Amanda Rouse, Business Systems Analyst (UTAB), provided us information from UTAB. The screens we saw are the ones the agents would use when claimants call. We tested three scenarios:

1. Claimant has worked less than 680 hours during base year, and
2. Claimant has worked more than 680 hours during base year, and
3. Claimant has worked 680 hours during base year.

Amanda provided a claimant for each scenario indicated above. See below:

1. We reviewed the Monetary Determination section of UTAB, Benefit Summary tab. The case number was 0-075-339-711. UTAB showed 81 hours in the base year and was listed as "Monetarily Ineligible". Weekly Benefit Amount (WBA) showed \$0.
2. We reviewed the Monetary Determination section of UTAB, Benefit Summary tab. The case number was 0-073-965-675. UTAB showed 720 hours in the base year and was listed as "Monetarily Eligible". WBA showed \$323.
3. We reviewed the Monetary Determination section of UTAB, Benefit Summary tab. The case number was 0-072-705-885. UTAB showed 680 hours in the base year and was listed as "Monetarily Eligible". WBA showed \$323.

For the three scenarios above, UTAB appropriately assessed eligibility of each claimant tested. **No issues noted.**

This key control is applicable to regular UI benefits. This does not apply to Pandemic Unemployment Assistance (PUA) benefits. PUA is a separate benefit program, that ended in September 2021, and provided a financial safety net to many people who did not qualify for regular unemployment, including:

- Self-employed people
- Independent contractors
- Part-time workers (with fewer than 680 hours)

ESD had a minimum payment that claimants received without documentation, however, ESD began validating self-employment or partial employment claims starting December 2020.

## **STEP 3: Understand General IT Controls**

We met with Zachary McInroy, Security Analyst, and Adarsh Jnawali, IS Governance, Compliance, & Risk Analyst, on May 13, 2024 to gain an understanding of general IT controls over the UTAB system.

## State of Washington

Any changes to the UTAB system flow must go through the pre-production (test) environment before they are implemented in the production (live) environment. Major changes that would change the architecture of the UTAB system require a review from the Office of Cyber Security. A change request would be filled out by the system owner and would be sent to the Security Team. The system owner would meet with the Security team to discuss the requested changes, provide architecture diagrams and to answer any questions. The Security team would then create a risk assessment and send it to the Office of Cyber Security for their review. The Office of Cyber Security will then issue a summary of the changes and this document will need to be signed by the system owner and other business leaders. After these approvals, the change will be communicated to other ESD departments and the Change Advisory Board so they can review the changes to determine if the change will affect other ESD IT systems. The Change Advisory Board has representatives from every major IT system at ESD. Any questions from the Board will be directed at the UTAB developers and this process helps work through any potential problems that were not thought of during the change request process. Once all this is completed, the work to implement the changes will begin.

Quality and security updates do not go through the change approval process mentioned above. Quality and security updates are regular updates that ESD makes to their software to remove any bugs that have been identified, and to correct any security vulnerabilities. As mentioned above, all changes must go through testing before going into production. The first stage of testing is performed by the QA Team. If the programming passes the initial testing with dummy data, the developer will request a migration to the staging environment, which is a mirror of the production environment (live) and uses real data. This testing process ensures that the changes function as intended using real world data. All changes to the system are recorded, including who made the changes. Once the changes have gone through the testing process, there is a UTAB team that will review the testing results and approve the changes for production. Once the UTAB team approves the changes for production, the Change Advisory Board will review the test results. If approved by the Board, ESD will schedule the changes to go to production.

Before the scheduled update to production, ESD has a plan in place in case the "go live" update has errors and a "roll-back" to prior code is required. Automated emails are sent to appropriate staff informing them of the date and time of the update. Once the changes have been implemented, there is another email that will state whether the changes have been successfully implemented or whether ESD is going to roll-back the change and re-schedule the update. Once the changes have been successfully implemented in production, there is a UTAB Team that will perform QA testing to ensure the implemented changes are functioning as intended (**Key Control #1**).

### **STEP 4: Confirm Key General IT Controls**

**Key Control #1 - All changes to the UTAB system must go through a standard change process, where changes are tested, reviewed and approved before migrating to production.**

We requested and received ESD's SQR screenshots for the most recent quality control update (SQR 12654), which was provided by Stephanie Eskesen, Audit Liaison. This update was requested by Wendy Yunker, Fraud Systems Management Analyst, on January 19, 2024, and was assigned to Jason Sikorski, Lead Applications Developer. The purpose of the update is to provide the ability to mark and add notes to claimant's eServices/Secure Access Washington (SAW) web sessions as potentially hijacked by bad actors to aid Investigators in reviewing web session activity without having to scour through past notes. As of the time the ticket was created, the development team had higher priority projects to work on, which is why the development took approximately 5 months. Development began on February 21, 2024, and was completed on June 3,

## State of Washington

2024. Jason's request to migrate to testing was approved by Matt Sleipness, Investigator 3 - On Project, who also completed the testing. Jason requested migration to the staging environment on June 3, 2024 which was approved by Mark Beck, FAST Contractor, on June 4, 2024. The update migrated to staging on June 5, 2024. Jason Sikorski requested the migration from staging to production on June 10, 2024 and Mark Beck approved the migration to production on June 10, 2024 and the update was migrated to production on June 12, 2024. We have confirmed that changes to the UTAB system must go through the standard process of development, testing, and approval to migrate between environments. **No issues noted.**

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **E.4.PR.G - Premiums and Claims**

*Procedure Step:* Key Control 2 (System Determination - Automated)

*Prepared By:* DRR, 6/14/2024

*Reviewed By:* SHW, 8/22/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To determine whether through UTAB and ESD's Fraud Unit, ESD runs initial and weekly claims through the discovery process before payment goes out (**Key Control #2 for UTAB system**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [[Risk Assessment](#)].

# State of Washington

## Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

#### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

## State of Washington

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity,*



## State of Washington

*different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

## State of Washington

Is there any exception situations where approval can be by-passed or waived?  
Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?  
Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?  
Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

## State of Washington

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

## State of Washington

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change*

## State of Washington

*management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

## State of Washington

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live*

## State of Washington

*production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

## State of Washington

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually*



## State of Washington

*implemented key controls).*

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

#### **Automated Interfaces:**

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

#### **Edit Checks:**

## State of Washington

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.

If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.

If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would*

## State of Washington

*normally be sufficient evidence to conclude that no further testing is necessary.*

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

### **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### **Manual vs. Automated Interfaces**

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules,

## State of Washington

such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors,

## State of Washington

rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An "**electronic signature**" can look like a handwritten signature that has been scanned and then pasted into an electronic document. The

## State of Washington

reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

### **Premiums and Claims - Rights & Obligations**

**Key Control 2 (Rights & Obligations - Automated):** Through UTAB and their Fraud Unit, ESD runs initial and weekly claims through the discovery process before payment goes out. The discovery process is when claims are run through a variety of cross matches and queries, both internally, with other agencies, and partners to identify and flag suspicious claims for identity verification.

The understanding for this system is documented above in the "Controls - UTAB" step.

### **STEP 1: Understand Automated Key Control**

The understanding for this automated key control is documented above in the "Controls -UTAB" step.

### **STEP 2: Confirm and Test Automated Key Control:**

On 5/23/2024, Amanda Rouse, Business Systems Analyst (UTAB), provided us screenshots from UTAB. We viewed screens from the UTAB user interface and a query from the UTAB database to show that the discovery process is being run before payment goes out.

Screenshots from the UTAB User Interface:

## State of Washington

### 1. Claimant with No Issues:

Claim ID: C9CD9S-010

Under customer screen we reviewed the Task - Cases Tab

Claim Registration - Create Claim: January 18, 2024

No Discovery issues noted.

We noted that the first payment was not made until February 6, 2024. **No issues noted.**

### 2. Claimant with Issue:

Claim ID: GNGWSS-001

Under customer screen we reviewed the Task - Cases Tab

Claim Registration - Create Claim: January 12, 2024

Non-Sep - Identity - Re-Determined:

The issue was initially created on January 12, 2024

An ID theft claim was made by an investigator on January 17, 2024.

A presumptive determination was issued on January 21, 2024.

We clicked on the non-sep - identity theft claim was made by an investigator on January 17, 2024. It stated that the claimant did not verify identity and the identity issue must be referred to OSI. The claimant did not respond to the letter that was sent in order to confirm their identity, so a presumptive determination was made on January 21, 2024 and their claim was denied.

Outcome: Deny

We noted that there were no payments made to the claimant. **No issues noted.**

### Query from the UTAB Database:

#### 1. Claim ID: C9CD9S-010

Discovery Process ran on January 18, 2024

Discovery score was 350

#### 2. Claim ID: GNGWSS-001

Discovery Process ran on January 12, 2024

Discovery score was 1,250

We determined that the discovery process was ran before payment was made, if applicable. **No issues noted.**

### **STEP 3: Understand General IT Controls**

We gained an understanding of general IT controls in the "Key Control 1 (System Calculation - Automated)" step here [[Key Control 1 \(System Calculation - Automated\)](#)].



# State of Washington

## **STEP 4: Confirm Key General IT Controls**

**Key Control #1 - All changes to the UTAB system must go through a standard change process, where changes are tested, reviewed and approved before migrating to production.**

We confirmed this key control as part of the "Key Control 1 (System Calculation - Automated)" step linked above.

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **E.4.PRG - Premiums and Claims**

*Procedure Step:* Key Control 3 (Manual - RSI Review)

*Prepared By:* DRR, 6/10/2024

*Reviewed By:* SHW, 7/31/2024

Purpose/Conclusion:

### **Purpose:**

To confirm UTAB sends a Request for Separation Information (RSI) form to the last employer, and when returned, is reviewed by the Adjudicator to confirm that the claimant worked for the employer and the reason for the separation (**Key Control 3 for the UTAB system**) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

## **Premiums & Claims - Rights & Obligations**

**Key Control 3 (Rights & Obligations - Manual):** When a claim is filed, UTAB sends a Request for Separation Information (RSI) form to the last employer (only covered employment) and any employer that has a separation issue and does not meet purge requirements. The returned RSI is reviewed by the assigned claim Adjudicator to confirm that the claimant worked for the employer and the reason for the separation.

The understanding for this system is documented above in the "Controls - UTAB" step.

### **1. Confirmation of Key Manual Control:**

On 5/23/2024, Amanda Rouse, Business Systems Analyst (UTAB), provided us information from the UTAB test environment. We reviewed screens to show that a Request for Separation Information (RSI) form is sent out before payment is made to the claimant. See below:

#### Regular UI - Disqualified:

Case Number: 0-075-095-568

Claim ID: 5GB7CX-001

Program Type: UI

Under the claim ID screen we reviewed the Task – Cases tab and noted that there was one separation case (excluding purge). See below:

Quiroga Law Office PLLC – RSI form was sent on March 29, 2024

The employer responded on April 8, 2024. The Adjudicator confirmed the employee worked for the employer on the claim.

The UI claim was denied, as the claimant quit for personal reasons.

Under the claim ID screen we reviewed the Benefits - Weekly Summary tab. We noted the following:

The claimant had not been paid, since they had a "Disqualified" status.

#### Regular UI - Not Disqualified:

Case Number: 0-075-356-495

Claim ID: JSVP59-004

Program Type: UI

Under the claim ID screen we reviewed the Task – Cases tab and noted that there was one separation case (excluding purge). See below:

Schuss Cafe – RSI form was sent on May 3, 2024

The employer did not respond to the RSI. ESD would expect an employer to fight the claim if the claimant was not employed by the employer. The Adjudicator's ultimate determination was to allow the separation and pay the claimant due to being un-employed through no fault of their own.

Under the claim ID screen we reviewed the Benefits - Weekly Summary tab. We noted the following:

The claimant had received their first payment on May 17, 2024, after the RSI form had been sent out.

# State of Washington

**No issues noted.**

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **E.4.PRG - Premiums and Claims**

*Procedure Step:* Key Control 4 (System Determination - Automated)

*Prepared By:* DRR, 6/14/2024

*Reviewed By:* SHW, 8/22/2024

Purpose/Conclusion:

### **Purpose:**

To determine whether the UTAB system properly assesses claimant's eligibility based on claimant's responses to the questions asked during weekly filing (**Key Control #4 for UTAB**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

Testing Strategy:

# State of Washington

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

## State of Washington

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for*

# State of Washington

*overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

## Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

## Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?



## State of Washington

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?  
Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?  
Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

## State of Washington

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

# State of Washington

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

## Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

## Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

## Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying*

## State of Washington

*communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

## State of Washington

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we*

## State of Washington

*would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

## State of Washington

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

# State of Washington

## **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **Automated Interfaces:**

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **Edit Checks:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.



## State of Washington

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

## State of Washington

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

## **Manual vs. Automated Interfaces**

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

## State of Washington

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

## State of Washington

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

## State of Washington

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

### **Premiums & Claims - Rights & Obligations**

**Key Control 4 (Rights & Obligations - Automated):** The UTAB system assesses claimant's eligibility based on claimant's responses to the questions asked during weekly filing.

The understanding for this system is documented above in the "Controls - UTAB" step.

### **STEP 1: Understand Automated Key Control**

The understanding for this automated key control is documented above in the "Controls -UTAB" step.

### **STEP 2: Confirm and Test Automated Key Control:**

On 5/23/2024, Amanda Rouse, Business Systems Analyst (UTAB), provided us screenshots from the UTAB test environment related to five questions that we expect to create an issue and put a claim on hold (pending) or contingently paid depending on the answer. The screenshots provided are the screens the agents would use when claimants call to file for weekly benefits.

A payment is on hold (pending) when there is an issue that arises for a new claimant filing a new claim. A claim is only contingently paid when claimants are on "continued claim status". This means that the claimant has previously filed a claim without any issues.

## State of Washington

1. Did you begin attending a school or training program?

The claimant answered **yes** to this and we expected an issue to be created (UI Claim Number QQ33GC-003).

Week Ending December 2, 2023: We noted that an issue was created for this claim. As this individual had an active claim and had been receiving benefit payments (continued claim status) in the weeks prior, the issue created did not automatically stop payment. We noted the activity tab shows the reason for the denial was due to school attendance, the claimant received a benefit decrease and the benefit payment was an overpayment.

2. Were you physically able and available for work each day of the week?

The claimant answered **no** to this and we expected an issue to be created (UI Claim Number K662BW-001).

Week Ending April 6, 2024: We noted there was an issue created for this claim. As this individual had an active claim and had been receiving benefit payments (continued claim status) in the weeks prior, the issue created did not automatically stop payment. Due to the hours available for work the claimant entered into the weekly claim, the claimant received a reduced benefit amount. Additional fact finding was completed on April 29, 2024, and it was determined the claim should be denied and the benefit payment was an overpayment.

3. Did you complete at least three job search activities and keep a written record as required?

The claimant answered **no** to this and we expected an issue to be created (CBP7RT-002).

Week Ending October 28, 2023: We noted there was an issue created for this claim and that this claim was denied. No payment was made to the claimant.

4. Did you refuse any offer of work?

The claimant answered **yes** to this and we expected an issue to be created (UI Claim Number 9RP24G-002).

Week Ending February 10, 2024: We noted there was an issue created for this claim and that this claim was adjudicated, and ultimately denied. No payment was made to the claimant after the denial.

5. Did you turn down a job offer, or fail to go to a job interview that you were referred to by WorkSource?

The claimant answered **yes** to this and we expected an issue to be created (UI Claim Number BMN7WB-001).

Week Ending July 8, 2023: We noted there was an issue created for this claim and that there has been a presumptive determination for this claim. The claim was denied and no payment was made to the claimant.

We looked at the Adjudicator tab, that shows the issue, which includes the source of where the issue originated (i.e. Weekly Claim), and the benefit week from and to date. An issue was created for each question as expected. **No issues noted.**

### **STEP 3: Understand General IT Controls**

We gained an understanding of general IT controls in the "Key Control 1 (System Calculation - Automated)" step here [[Key Control 1 \(System Calculation - Automated\)](#)].

# State of Washington

## **STEP 4: Confirm Key General IT Controls**

**Key Control #1 - All changes to the UTAB system must go through a standard change process, where changes are tested, reviewed and approved before migrating to production.**

We confirmed this key control as part of the "Key Control 1 (System Calculation - Automated)" step linked above.

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **E.4.PRG - Premiums and Claims**

*Procedure Step:* Key Control 5 (System Calculation - Automated)

*Prepared By:* DRR, 6/18/2024

*Reviewed By:* RKM, 11/8/2024

Purpose/Conclusion:

### **Purpose:**

To determine whether the UTAB system automatically and accurately calculates the unemployment benefit payment amounts (**Key Control #5 for UTAB**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:



# State of Washington

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

## State of Washington

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and*

# State of Washington

*transaction processing controls.*

## Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

## Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

## State of Washington

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

# State of Washington

## Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

## Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

# State of Washington

## Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

## Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

## Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

## State of Washington

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables*

## State of Washington

*or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*



## State of Washington

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

## State of Washington

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3

## State of Washington

is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### Software Calculation:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Automated Interfaces:

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

## State of Washington

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Information Technology](#) Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

#### Manual vs. Automated Interfaces

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the*

# State of Washington

*following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process

## State of Washington

to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm



# State of Washington

with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **Premiums & Claims - Valuation**

**Key Control 5 (Valuation - Automated):** The UTAB system automatically and accurately calculates the unemployment benefit payment amounts.

The understanding for this system is documented above in the "Controls - UTAB" step.

## **STEP 1: Understand Automated Key Control**

The understanding for this automated key control is documented above in the "Controls -UTAB" step.

## **STEP 2: Confirm and Test Automated Key Control:**

Per [RCW 50.20.120](#), the total amount of maximum benefits payable on the claim is found by taking the smaller of 1/3 of the total gross wages in all four quarters of the base year or 26 times the weekly benefit amount (WBA) determined.

The calculation uses two limits for the maximum benefits amount/payable (MBA):

WBA x 26

Total Base Wages / 3

We reviewed the UTAB screen and re-performed the calculations for instances of both limits as detailed below:

On 5/23/2024, Amanda Rouse, Business Systems Analyst (UTAB), provided us with information to test automated calculations in UTAB. See

## State of Washington

details below:

### **[WBA x 26] Maximum Benefits Amount/Payable**

1) We reviewed case number 0-073-792-880. We reviewed the Monetary Determination screen, Maximum Benefit Amount (MBA) & Weekly Benefit Amount (WBA) Calculations tab, in UTAB:

High Quarter Wage 1	High Quarter Wage 2	High Quarter Wage Avg
\$53,035.38	+	\$51,560.58
<hr/>		=
2		\$52,297.98
High Quarter Wage Avg.	State Multiplier from RCW	Weekly Benefit Amount
\$52,297.98	X	0.0385
		=
		\$1,019
Total Base Wages		Max Benefits Payable
\$201,451.71	/3	
		=
		\$67,150.57
Weekly Benefit Amount		Max Benefits Payable
\$1,019	X 26	
		=
		\$26,494

The MBA was \$26,494. The system correctly calculated the MBA using the WBA times 26 as it produced the smaller MBA.

### **[Total Base Wages / 3] Maximum Benefits Amount/Payable**

2) We reviewed case number 0-071-932-487. We reviewed the Monetary Determination screen, MBA & WBA Calculations tab, in UTAB:

High Quarter Wage 1	High Quarter Wage 2	High Quarter Wage Avg
\$8,778.48	+	\$3,477
<hr/>		=
2		\$6,127.74
High Quarter Wage Avg.	State Multiplier from RCW	Weekly Benefit Amount
\$6,127.74	X	0.0385
		=
		\$323
Total Base Wages		Max Benefits Payable

## State of Washington

$$\$12,255.48 \quad /3 \quad = \quad \$4,085$$

Weekly Benefit Amount				Max Benefits Payable
\$323	X 26	=		\$8,398

The MBA was \$4,085.00. The system correctly calculated the MBA by using the total base wages divided by three as it produced the smaller amount.

### **STEP 3: Understand General IT Controls**

We gained an understanding of general IT controls in the "Key Control 1 (System Calculation - Automated)" step here [[Key Control 1 \(System Calculation - Automated\)](#)].

### **STEP 4: Confirm Key General IT Controls**

**Key Control #1 - All changes to the UTAB system must go through a standard change process, where changes are tested, reviewed and approved before migrating to production.**

We confirmed this key control as part of the "Key Control 1 (System Calculation - Automated)" step linked above.

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **E.4.PRG - Premiums and Claims**

*Procedure Step:* Key Control 6 (Manual - UTAB to AFRS Reconciliation)

*Prepared By:* DRR, 6/27/2024

*Reviewed By:* SHW, 8/22/2024

Purpose/Conclusion.\*

#### **Purpose:**

To confirm the Treasury Manager or Assistant Treasury Manager reviews reconciliations and indicates reconciling items were accurate with tickmarks to ensure AFRS data is accurate and complete (**Key Control #6 for UTAB**) in order to assess control risk.

# State of Washington

## **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or*

## State of Washington

*detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Premiums & Claims - Completeness**

**Key Control 6 (Completeness - Manual):** The Treasury Manager or Assistant Treasury Manager reviews reconciliations and indicates reconciling items were accurate with tickmarks to ensure AFRS data is accurate and complete.

The understanding for this system is documented above in the "Controls - UTAB" step.

#### **1. Confirmation of Key Manual Control:**

This key control is tested as part of Cash and Cash Equivalents at: [[Cash & Cash Equivalents](#)]. ***No issues noted.***

We received the "January 2024 Monthly AFRS JV to Webi TEMPLATE with all GLs" spreadsheet from Meghan Phelps, Treasury Manager. We reviewed the "6510" (Cash Expenditures/Expenses) tab for fund 620. On this tab, we noted on the left it stated "Journal to AFRS" and on the right it stated "Journal to UTAB". The beginning balance of \$815,873,479.33 was the same for both sides of the spreadsheet. Both sides of the spreadsheets had entries that were made to both AFRS and UTAB. The entries on the AFRS side were directly linked to another tab that had the entry for JV 54007804. There was no adjustment needed since AFRS and UTAB had the same entries made this month. The ending balance of \$1,004,538,468.68 matched both on the AFRS and UTAB side for a variance of \$0. Additionally, we noted this spreadsheet was prepared by Son Pham, Fiscal Analyst 4 on February 20, 2024 and reviewed by Shelly Peterson, Assistant Treasury Manager on February 29, 2024. Per Shelly Peterson, Assistant Treasury Manager, this document is too large to convert into a PDF, or sign each page individually, so the preparer and reviewer of the document sign off on the "Federal" tab. **No issues noted.**

Note: The ending and beginning balances for AFRS and UTAB is large. This is due to biennial adjustments to the income statement. OFM rolls balances over after the fiscal year and ESD shows that amount on their reconciliation for expenditures. ESD uses the reconciliation as back-up for their entry into UTAB at fiscal year-end.

#### **2. Preliminary Control Risk Assessment**

## State of Washington

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **E.4.PRG - Premiums and Claims**

*Procedure Step:* Key Control 7 (Manual - UTAB Claims Accrual)

*Prepared By:* DRR, 10/1/2024

*Reviewed By:* RKM, 11/7/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm the Treasury Manager, or Assistant Treasury Manager will create the journal voucher to record the claims accrual and the Treasury Director, or Treasury Manager will review the journal voucher and calculation to ensure that the calculation is complete and correct (**Key Control #7 for UTAB**) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented*

## State of Washington

*key controls).*

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).



## State of Washington

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

## **Premiums & Claims - Completeness/Valuation**

**Key Control 6 (Completeness/Valuation - Manual):** The Treasury Manager, or Assistant Treasury Manager will create the journal voucher to record the claims accrual and the Treasury Director, or Treasury Manager will review the journal voucher and calculation to ensure that the calculation is complete and correct

The understanding for this system is documented above in the "Controls - UTAB" step.

### **1. Confirmation of Key Manual Control:**

We received the "FY 2024 UI Appeal Accrual Entry" spreadsheet from Meghan Phelps, Treasury Manager. In this spreadsheet were various tabs which included screenshots of the "Total Issues and Outcomes" UTAB reports, a screenshot of the U.S. Dept. of Labor's monthly claims data used to calculate the accrual amount of \$203,477,783.17. We reviewed JV 54014803 prepared by Meghan Phelps, Treasury Manager on August 23, 2024 "To record an accrual for estimated unemployment insurance benefit claims incurred but not paid as of June 30, 2024", and was approved by Ibrahim Dembele, Treasury Director on August 23, 2024. The accrual amount calculated ties to the JV amount without exception. **No issues noted.**

Additionally, we re-calculated the accrual amount without exception here [[Claims Accrual Testing](#)]. **No issues noted.**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **E.4.PR.G - Premiums and Claims**

*Procedure Step:* Risk Assessment

*Prepared By:* DRR, 7/22/2024

*Reviewed By:* CJG, 11/21/2024

# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

*General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

*Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

## State of Washington

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

## State of Washington

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Completeness – **High**

Rights & Obligations – **High**

Valuation – **High**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**UTAB** – Completeness, Rights & Obligations, and Valuation

## State of Washington

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Completeness – **High**

Rights & Obligations – **High**

Valuation – **High**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

#### **Completeness:**

We will select a sample of cash draws and ensure that bank deposits are complete and tie to UTAB.

#### **Valuation and Rights & Obligations:**

We will select a sample of FY24 benefit payments and perform the following:

Recalculate the benefit payments for selected accounts (Valuation)

Verify hours worked during the base year to determine the State's obligation (Rights & Obligations)

Determine whether the Department verified the claimant's ID prior to payment (Rights & Obligations)

Determine whether the Department sent a Request for Separation Information (RSI) form to the claimant's employer prior to payment (Rights & Obligations)

Determine whether the claimant is eligible for benefits (Rights & Obligations)

#### **Valuation/Completeness:**

We will determine if the yearly claims accrual estimate is complete and calculated correctly.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

# State of Washington

## E.4.PRG - Premiums and Claims

*Procedure Step:* Substantive Test

*Prepared By:* DRR, 9/24/2024

*Reviewed By:* CJG, 11/21/2024

### Purpose/Conclusion:

#### **Purpose:**

To determine whether all expenses/expenditures incurred during the period were reported.  
To determine whether the entity would have legal authority to make reported expenses/expenditures.  
To determine whether expenses/expenditures were reported at properly valued or calculated amounts.

#### **Conclusion:**

We determined all expenses/expenditures incurred during the period were reported.  
We determined the entity had legal authority to make reported expenses/expenditures.  
We determined expenses/expenditures were reported at properly valued or calculated amounts. **No issues noted.**

### Testing Strategy:

The following is a list of **considerations** for testing the completeness assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

#### **Detail Roll-Up**

Compare totals from general ledger to accounts payable, payroll or other subsidiary software modules.  
Review the government's reconciliation of general ledger to subsidiary systems.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

#### **Cut off / Improper Expense Recognition**

# State of Washington

Scan expenditures recorded 1-3 months before and/or after fiscal year end (expenditures not charged to the current period). Based on the scan, test selected or sampled expenditures to determine if the expense should have been reported in the current period. Inquire with AP clerks regarding invoices held, but not entered as of year-end (ie: due to pending litigation or disputes).

## **Unrecorded Expenses**

If the entity reconciles recorded revenues and expenses to bank activity, then reviewing monthly reconciliations and evaluating or testing reconciling items.

## **Accounts Payable**

If entity uses a warrant clearing account for vendor payments, review the entity's year-end reconciliation of recorded vendor payments with disbursements from the clearing account.

Review edit check reports from the AP system that might indicate missing payments.

## **Payroll**

If entity uses a payroll clearing account, review the entity's year-end reconciliation of recorded payroll with disbursements from the payroll clearing account.

Perform an expected payroll test by taking the prior audited payroll amount and adjusting it for expected changes.

*The analysis should consider changes in employees, COLA increases, salary scale increases if automatic, changes wages or benefits due to changes in policy or union negotiations changes, etc. Sources for these expectations should be obtained apart from the payroll records that are being tested. Since the auditor would not expect to be able to precisely predict payroll, the auditor should document a reasonable range within which actual payroll is expected to vary from the auditor's prediction.*

If the board directly approves salaries for a significant amount of employees, verify whether the actual salaries for these employees is within an expected reasonable range of the approved salary.

For small entities, compare payroll by employee to known employees per observation, organization charts or a phone list.

Review edit check reports from the payroll system that might indicate missing payments.

## **Unrecorded Liabilities**

Evaluate liabilities directly related to expenses for completeness. See the completeness steps for current and non-current liabilities for testing considerations.

*For example, if the entity reports a self-insurance liability, the auditor might evaluate whether the change in the liability (and related expense) was determined and recorded. If no liability was reported, then the auditor might determine whether such a liability (and associated expense) should have been reported.*



# State of Washington

**OPEB** - auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

## **Removing Expenses from Accounting Records**

Search for manual journal entries that credit (decrease) expenditures. Consider testing selected transactions.

Identify transactions that void, cancel, or manually adjust transactions in subsidiary AP or payroll systems. Auditors may conclude that the total amount of such transactions are trivial or otherwise reasonably small. Or auditors may sample or select transactions for testing.

*Also see considerations under the "Not recording expenses" section.*

## **Interfund Expenses**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

The following is a list of **considerations** for testing the valuation assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests:

Verify that payroll calculations are correct.

If not already covered as part of control testing, verify that payroll software used correct rates.

If not already covered as part of control testing, verify that accounts payable software used correct rates for calculating sales tax.

Review calculation of any estimated expenses.

Review related-party transactions to determine whether expense/expenditure transactions were correctly calculated.

## **Landfill Closure & Post-Closure Expenses**

*See the valuation testing strategy for non-current liabilities..*

**OPEB** - Auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - Auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

The following is a list of **considerations** for testing the rights and obligations assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## State of Washington

Review selected expenses/expenditures to determine whether the entity had legal authority to make the payments or incur the liability.

If disbursements for different entities are made out of the same bank account, review the entity's reconciliation of accounting records to disbursements to verify that only expenditures of the entity were reported by that entity.

Compare vouchers audited and certified by the auditing officer to the warrant register or review documentation for selected or sampled vouchers to determine whether expenses/expenditures were audited and certified in accordance with RCW 42.24.080.

Compare board-approved vouchers to the warrant register or review documentation for selected or sampled vouchers to determine whether expenses/expenditures were properly approved by the governing body.

Test selected or sampled transactions for compliance (allowability, eligibility, etc) with applicable restrictions or requirements.

*NOTE: this test may be combined with expenditure tests for other attributes. For example, expenditure testing for accountability or single audit purposes would normally also be considered testing for the rights & obligations assertion.*

### Expenditures related to Joint Ventures or Other Arrangements

Review forming documents and agreements to verify expenditures for obligations of the venture.

**OPEB** - Auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - Auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

Guidance/Criteria.*
---------------------

#### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS 3.6.13 Utility Tax (*applies only to cities*)** - should be accounted for as a revenue in the general fund (3164000) and expenditure in the utility fund (53P0040), if the utility passes the tax on to its customers then the additional charges should be recognized as revenue (343P000) directly in the utility fund not in the general fund

#### **BARS 3.8.6 Use of Payroll and Claims Funds**

#### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

# State of Washington

## **BARS [3.8.6](#) Use of Payroll and Claims Funds**

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.8.5](#) Voucher Certification and Approval** - prescribes the form and manner of the audit and certification

## **BARS [3.8.6](#) Use of Payroll and Claims Funds**

**RCW [42.24.080](#)** - describes statutory audit, certification and approval requirements

Record of Work Done:

### **Substantive tests performed to meet the Completeness assertion:**

#### Daily Cash Draws:

We used the Nonstatistical Sample of Population 365 or less spreadsheet [[Daily Cash Draw Testing](#)] with a tolerable misstatement and assurance levels dictated by the material balance workpaper for a planned sample size of 24. We used the random number generator to randomly select 24 sample dates throughout FY24.

We obtained UTAB general ledger postings (Daily Draw Worksheet section), all supporting documentation (UTAB Daily Draw Adjustments sections and AFRS posting), and payment transaction confirmations (US Bank account ending 9548 statements) from Stephanie Eskesen, ESD External Audit Liaison.

We performed the following procedures:

- We tested the general ledger posting for the presence of a signature indicating supervisory review.

- We tested that the review was done in a timely manner.

- We manually calculated the amounts on the general ledger posting from the supporting documentation (adjustments) to ensure that the worksheet was programmed correctly and to develop an expectation of the results of supervisory review.

- We confirmed that the US Bank confirmation tied to the total in UTAB.

See substantive testing at: [[Daily Cash Draw Testing](#)]. ***No issues noted.***

#### Bank Reconciliations:

We rely on testing of the bank reconciliations related to benefits at: [[Cash & Cash Equivalents](#)].

# State of Washington

## Claims Accrual:

See testing: [[Claims Accrual Testing](#)]. Meghan Phelps, Treasury Manager, provided us with excel worksheet "FY 2024 UI Appeal Accrual Entry GL5118" in which we noted that ESD used UTAB "Total Issues and Outcomes" reports and U.S. Department of Labor data in order to calculate the yearly estimate of claim accrual.

The UTAB reports were used to find the number of allowable cases, the "total bucket" of cases (all cases less any open cases at the end of the fiscal year), and the amount of open cases. The reports aren't labeled with dates, but both reports are for issues created from 7/1/23 through 6/30/24. The difference between the two reports is that the one of the reports is for issues closed from 7/1/23 through 6/30/24, while the other report is for issues closed from 7/1/24 through 8/23/24. ESD uses the first report to identify the amount of claims in the backlog that were allowed. ESD then runs the second report, with a date range of 7/1/24 through the day before they calculate the estimate (8/23/24). They assume these cases were in backlog as of 6/30/24. They apply the ratio calculated from the first report to estimate how many open claims from the second report will most likely be allowed and therefore paid out. We determined that this is a reasonable way to determine the ratio of open cases that will be allowed. We ran these reports in UTAB and determined that the dataset is complete. **No issues noted.**

Finally, we noted that ESD used monthly program and financial data retrieved from the U.S. Department of Labor's website in order to arrive at the "weekly amount" and "# of weeks" figures used in the calculation of the yearly estimate. We retrieved this data from the website ourselves and determined that ESD used all monthly program data from FY24. We determined that this dataset was complete.

On the "SAO Accrual Re-Calc" tab, we used the two UTAB "Total Issues and Outcomes" reports, and the U.S. DOL data to recalculate the claims accrual.

On the "SAO-ESD Accrual Calc. Compare" tab, we compared the total estimated accrual amount per ESD's workbook, to our own recalculation and noted they tied without exception. We then confirmed the accrual tied to the JV posted to AFRS. **No issues noted.**

## **Substantive tests performed to meet the Valuation assertion:**

### UI Benefits:

We used the Financial Audit Substantive Statistical Sample spreadsheet with a tolerable misstatement of 7.5%, and high assurance levels, and we arrived at a planned sample size of 39. We determined we would test 19 additional sample items due to the risk associated with claims payments. Priscilla Soh, IT Auditor (Team IT Audit), randomly pulled these samples using the benefit week payment date. The data is received by quarter, so we asked them to randomly select the following:

- 15 claimants from Q3 2023 (July - Sept 2023)
- 15 claimants from Q4 2023 (Oct - Dec 2023)
- 14 claimants from Q1 2024 (Jan - March 2024)
- 14 claimants from Q2 2024 (April - June 2024)

## State of Washington

To verify that UTAB is calculating benefit payments and maximum benefits payable accurately, we reviewed screens within UTAB and recalculated benefit payments for the sample. We reviewed the calculations for the following:

Weekly Benefit Amount (WBA)

We added together the gross wages in the two highest quarters during the period, divided by 2, and then multiplied by 0.0385 (RCW 50.20.120).

Earnings Deduction (if applicable)

If the claimant has earnings during the week, ESD deducts part of the earning from the WBA.

We take the gross earning minus \$5.00 multiplied by 75%. All deductions are rounds up to the next highest dollar.

Intercepts (if applicable)

This is money taken out of the benefit payment for the following reasons:

Income Tax Withholding

Repaying a Debt to ESD

Child Support

Maximum Benefits Payable

The total amount of benefits potentially payable on the claim is found by taking the smaller of:

26 times the claimants's weekly benefit amount or

1/3 of the total gross wages in all four quarters of the claimant's base year

See substantive testing performed at: [Regular UI Claims Testing]. **No issues noted.**

Claims Accrual [Claims Accrual Testing]:

On the "SAO Accrual Re-Calc" tab, we recalculated the "weekly amount" and "# of weeks" figures used to calculate the yearly estimate of claim accruals. We were able to properly recalculate these figures using data retrieved from the U.S. Department of Labor's website. We used these figures to recalculate the total estimated accrual amount. We were able to properly recalculate the amount using the "Total Issues and Outcomes" Reports from UTAB, the "average duration of benefits (weeks)" amount, and the "average WBA" amount without exception. **No issues noted.**

**Substantive tests performed to meet the Rights & Obligations assertion:**

UI Benefits:

We used the Financial Audit Substantive Statistical Sample spreadsheet with a tolerable misstatement of 7.5%, and a high assurance level, this arrived us at a planned sample size of 39. We determined we would test 19 additional sample items due to the risk associated with claims payments. Priscilla Soh, IT Auditor (Team IT Audit), randomly pulled these samples using the benefit week payment date. The data is received by quarter, so we asked them to randomly select the following:

15 claimants from Q3 2023 (July - Sept 2023)

15 claimants from Q4 2023 (Oct - Dec 2023)

14 claimants from Q1 2024 (Jan - March 2024)

# State of Washington

14 claimants from Q2 2024 (April - June 2024)

We reviewed screens within UTAB to verify the following:

If ESD verified the claimant's ID before payment was sent.

If ESD verified the claimant's hours worked during the base year, which determines the claimant's eligibility and ESD's obligation to pay.

If ESD sent a Request for Separation Information (RSI) form before paying the claimant.

If the payment is allowable.

See substantive testing performed at: [[Regular UI Claims Testing](#)]. ***No issues noted.***

## E.4.PR.G - Premiums and Claims

*Procedure Step:* Sample Methodology

*Prepared By:* PS, 8/7/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion.:

### **Purpose:**

To randomly selected samples from UTAB benefits paid during FY2024.

To provide the total amount and total number of transactions for FY2024.

### **Conclusion:**

Sample population are provided to audit team in Excel.

Testing Strategy.:

Guidance/Criteria.:

# State of Washington

Record of Work Done:

## **Import UTAB Data**

IT Audit emailed Stephanie Eskesen, ESD External Audit Liaison, and Samuel Havens, ESD Reporting, Accessibility, and Performance Manager, to request for UTAB data. This included the UTAB benefit payments, base year employer data and base year wage data.

The email was sent on 5/1/2024 to request fiscal year 2024 data. ESD provided the fiscal year 2024 UTAB data files in .csv format on 7/23/2024. The files were sent to SAO via the WaTech secure file transfer site (MFT.wa.gov). Files were saved to the SAO network drive and imported into SQL database. We have confirmed the record count of each file to the record count provided by ESD staff. No exception. We had also performed procedures at Reasonableness UTAB 2024 and have determined that the data are reasonable.

## **Document Test Objective**

This request was submitted by Team FA via Helpdesk 68024.

1. To randomly select 59 UTAB payment samples for testing as follow:
  - 15 payments from Q3-2024 (July - Sept 2023)
  - 15 payments from Q4-2024 (Oct - Dec 2023)
  - 14 payments from Q1-2024 (Jan - March 2024)
  - 14 payments from Q2-2024 (April - June 2024)
2. Provide the total number of payments and total dollars of UTAB payment population for FY2024.

## **Methodology**

We will randomly select samples from the UTAB UI benefit paid during the fiscal year 2024. As we perform our testing, we will make adjustments to this plan as necessary.

## **Queries**

The queries to complete the sample selection are at Testings UTAB 2024.

## **Reasonableness**

The reasonableness of test results has been performed and documented in the above queries. Based upon our checks, we consider our test results to be complete and reasonable.

## **Results**

# State of Washington

In fiscal year 2024, there are 2,848,409 UTAB payments for a total amount of \$1,716,586,963.76. This includes all entitlement types. The samples are provided to audit team in an Excel spreadsheet, !2024\_UTAB\_Samples.xlsx. The results provided contain CONFIDENTIAL DATA.

## F.1.PR.G - Claims and Judgments Payable

*Procedure Step:* Summary & Conclusion

*Prepared By:* EZM, 10/11/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or*



## State of Washington

*RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the **Permanent File** folder or assessment of control risk?
  - If circumvention, the **Management Override of Controls** step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and*

## State of Washington

*quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done.:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

**(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

No, the results of substantive tests do not indicate a need to modify our risk assessment.

**(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

Yes, the quality and quantity of evidence obtained was sufficient and appropriate.

### **F.1.PRG - Claims and Judgments Payable**

*Procedure Step:* Understanding of Line Item

*Prepared By:* EZM, 9/13/2024

*Reviewed By:* RKM, 10/2/2024

Purpose/Conclusion.:

# State of Washington

## **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

## State of Washington

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria:

Record of Work Done:

#### **(1) Prior Audit Exceptions:**

We noted **the following** prior audit exceptions:

Claims Data Accuracy - We reported an exit item due to the fact that HCA did not have a documented process in place to review the accuracy of claims data provided to their external actuary, Milliman. Milliman uses this data for the SEBB Receivables Risk Adjustment calculation and the incurred but not reported (IBNR) liability. HCA relies on Milliman's procedures alone to determine these balances, but Milliman does not audit the claims data used in these calculations and relies on HCA and its vendors to provide accurate data and information. We recommended that HCA perform and document a review of accuracy of key claims data used in actuary calculations for receivables and the IBNR liability.

We inquired with Sara Whitley, ERB Finance Manager, about this prior audit issue on April 26, 2024, and she informed us that there's sections of HIPPA that restrict the "plan sponsor" (HCA) from reviewing claims data passed directly from "group health plans" (third party administrators [TPA]). Specifically, these sections are [45 CFR 164.504, sections f\(2\) and \(3\)](#). Sara stated that the Authority contracts with Milliman to check for reasonableness of the raw claims data, that the Authority depends on TPAs to provide accurate claims data to Milliman, and as a compensating control, HCA compares claims reports from TPAs and compares the amounts in those reports to prior period amounts to ensure that trends are aligning with the Authority's expectations (see our control understanding and the confirmation work we did for key control #1 for more details on this last item). Considering that HCA is not allowed to review the claims data in detail, per HIPPA, and considering HCA's compensating control of reviewing TPA

## State of Washington

reports to ensure the claims amounts align with HCA's expectations, we've determined that it's reasonable for HCA to not review key claims data in detail. **No issues noted.**

Claims and Judgments Payable Error - We issued a verbal recommendation due to the fact that HCA and OFM understated the IBNR liability by \$8.645 million. Claims and Judgments Payable in the Health Insurance Fund within Note 7 (Long Term Liabilities) was also affected by this error by the same amount. We recommended that HCA correct this error and thoroughly review any IBNR adjustments for accuracy before posting. We also recommended that OFM work together with HCA during the concluding process to ensure note disclosures are accurate.

When we communicated this issue to Kelly Diaz, OFM Statewide Accountant, she informed us that this error would be corrected in FY24 with a prior period adjustment. We requested and received documentation from William Sogge, External Audit Liaison, and Rita Homan, Deputy Accounting Section Manager, showing that this prior period adjustment was performed in FY24, and when we analyzed the adjustments made (see [Adjustments to Correct Prior Year Understatement]), we found that the \$8.645 million understatement was fully corrected. **No issues noted.**

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [Line Item Lead Sheet]. See understanding of HCA's Employee Retiree Benefits (ERB) operations at [Health Insurance Activities Updated 2024].

The Claims and judgements payable balance is made up of HCA's incurred but not paid (IBNP) liability. This estimate is required for all self-insurance plans in Washington State and ensured solvency requirements. This liability is the estimate of self-insured medical, pharmaceutical, and dental claims that existed at the end of the period but have not been processed (billed) by HCA's third party administrators (TPAs), Regence (medical), MODA (pharmaceutical), and Delta Dental (dental). The estimate is prepared from quarterly actuary studies performed by Milliman using Regence, MODA, Delta Dental and HCA data. The estimate amount is provided to HCA through a quarterly memo. The estimate is typically 7% of rolling annual medical and pharmaceutical claims and 4% of dental claims for all of HCA's self-insured plans offered through Uniform Medical Plans offered to PEBB and SEBB subscribers. This balance acts as an accrual account for premiums and claims.

#### *ACFR Database*

We performed an analysis to review the composition of this ACFR line item. Total claims and judgments payable (GL\_Sort Code = NY) for FY23 at HCA were \$164,037,000, see [Interim Planning Significant Account Matrix] for details. We analyzed the reserve amounts in the line item lead sheet and identified fund 473 (SEBB) and 730 (PEBB) in GL account 5119 make up the balance of this line item with an insignificant portion attributed to OFM fund FFJ (year-end entry prepared by OFM).

We analyzed the reserve amounts and noted that the fund percentage compositions from 2023 were in line with 2022. There were dollar amount decreases in FY23 with fund 473 decreasing approximately 8 percent and fund 730 decreasing approximately 34 percent with a total decrease to this line item of approximately 32% from 2022 to 2023.

# State of Washington

## **(3) Updates to Significant Account Matrix:**

None.

## **F.1.PR.G - Claims and Judgments Payable**

*Procedure Step:* Controls - Actuarial Report

*Prepared By:* EZM, 5/6/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

# State of Washington

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable).

## State of Washington

Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls in the Actuarial Report address the following balance(s):

Claims and Judgements Payable - Current



# State of Washington

For the following assertions:

Valuation - Estimated claim payables (incurred but not reported liability) may be under-reported or not supported by amounts determined by actuaries; HCA used actuaries that were not creditable or lacked experience (educational and professional) to determine estimate; assumptions based on unaudited attestations made by HCA were not accurate (e.g. information relied on by Milliman did not reflect actual operations or benefits provided); and claim history information provided to Milliman was not complete (i.e. multiple sources of claims)

## **Gain an Understanding of Internal Controls**

We gained an understanding over the incurred but not reported (IBNR) with the following HCA staff on 4/26/2024:

Rita Homan, Deputy Accounting Section Manager  
Sara Whitley, ERB Finance Manager  
Lisa Kolle, PEB Accounting Manager  
Grant Stromsdorfer, Pay1 Mainframe Support  
Samantha Zimmerman, Internal Control Officer  
William Sogge, External Audit Liaison

HCA used Milliman for actuary services for operating the PEBB and SEBB Uniform Medical Plans (medical and dental). We performed the "Rely on Specialist" step in TeamMate to assess the competence, capabilities, and objectivity of the Milliman actuaries. See the Rely on Specialist step here [[Rely on Specialist](#)]. Milliman provides HCA a quarterly memo that summarizes the calculations for the incurred but not paid (IBNP) estimate using raw claims feed data from third-party administrators including Regence, MODA and Delta Dental and census data from HCA.

Due to HIPPA compliance rules as the plan sponsor and employer, HCA has limited access to the raw claims feeds from the third-party administrators. To ensure the amounts reported by the third-party administrators to Milliman are complete and accurate, HCA reviews multiple reports and compares them to prior periods to ensure that trends are aligning with expectations (**Key Control #1 - Manual - Valuation**). Some of these reports are the weekly "tracker" (internally generated) that includes the lump sum claims amounts due to Regence for medical claims, Regence Monthly Operations Report, and the MODA Rebate Report. The Regence Monthly Operations Report provided by Regence includes a tracking of claims processed to date as well as a claims inventory, claims incurred but not yet paid, and general claims seasonality for both PEBB and SEBB claims. HCA often shares this report with Milliman to ensure their amounts are in alignment with claims that Regence is reporting for the period. One of the reports that HCA reviews is the MODA Rebate Report provided by MODA, which details the projected rebate amounts, and rebates to be received for the pharmacy benefit. This report is reviewed and compared to what the Employee Retiree Benefits (ERB) accounting department and Milliman have recorded and is also shared with Milliman to ensure the amounts are in alignment with what MODA is reporting.

HCA meets with Milliman approximately once a week to update assumptions, projections, and various other items that may affect the IBNP estimate. After the end of the quarter, the ERB team and Milliman meet to discuss trends, drivers of assumptions and compare the memo to prior

## State of Washington

quarters before Tanya Duel, Section Manager, approves the memo (**Key Control #2 - Manual - Valuation**). Milliman will often provide a draft memo for discussion before providing the finalized memo, but due to conflicting timelines with receiving insurance carrier data, this is not always possible. The ERB finance team has full discretion to request updates to the memo if needed. If updates to the memo are necessary, Sara Whitley, ERB Finance Manager, would notify Milliman and the ERB accounting department and provide them with the updated memo. The ERB finance team consists of the following: Tanya Deuel, Section Manager; Sara Whitley, ERB Finance Manager; Molly Christie, Fiscal Information Data Analyst; Izzy Uong, Fiscal Information Data Analyst, and Kodi Campbell, Fiscal Information Data Analyst,

After the ERB Finance approves the memo, the memo is emailed to Katherine Plaquet, Fiscal Analyst 5, in the accounting department. Quarterly, Katherine prepares the journal voucher based on the IBNR summary charts in the Milliman memo. Rita Homan, Deputy Accounting Section Manager, or Lisa Kolle, ERB Accounting Manager, would review and post the journal voucher to ensure amounts were accurate and supported by the actuary memo (**Key Control #3 - Manual - Valuation**).

Note: HCA called the IBNP liability the IBNR liability. IBNP and IBNR were used interchangeably.

### **How Transactions are Recorded in AFRS:**

General journal vouchers were used to make quarterly adjustments to the IBNR estimate. A Fiscal Analyst 5 prepares the JV using the IBNR summary charts in the Milliman memo, and the Deputy Accounting Manager, or the PEB Accounting Manager would review and approve the JV.

### **Key Controls are as Follows:**

- Key Control #1: Valuation - The ERB Finance Team reviews multiple reports, such as their internal weekly paid claims tracker, Regence Monthly Operations Report, and MODA Rebate Report and compares them to prior periods to ensure that trends are aligning with expectations and that the amounts reported by third-party administrators to Milliman are complete and accurate.
- Key Control #2: Valuation - Milliman calculates and prepares the memo that summarizes the calculations for the incurred but not paid (IBNP) estimate in accordance with the data provided by Regence, MODA, Delta Dental and HCA, then meets with the ERB finance team to discuss the memo and compare it to prior quarters before the ERB Section Manager approves it.
- Key Control #3: Valuation – Quarterly, a Fiscal Analyst 5 prepares the journal voucher based on the IBNR summary charts in the Milliman memo. The Deputy Accounting Section Manager reviews the journal vouchers to adjust the incurred but not reported liability to ensure the amount is supported by the memo from Milliman, HCA agrees with the conclusions and analysis in the memo, and the IBNR amount is correctly calculated.

### **Noted Weaknesses are as Follows:**

None.

# State of Washington

## F.1.PR.G - Claims and Judgments Payable

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* EZM, 5/6/2024

*Reviewed By:* RKM, 5/29/2024

Purpose/Conclusion:

**Purpose:**

To confirm whether the ERB Finance Team reviews their internal weekly paid claims tracker, Regence Monthly Operations Report, and MODA Rebate Report to ensure that trends are aligning with expectations and that amounts reported by third-party administrators to Milliman are complete and accurate (key control #1 for Actuarial Report) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

## State of Washington

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

## State of Washington

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #1 (Valuation):** The ERB Finance Team reviews multiple reports, such as their internal weekly paid claims tracker, Regence Monthly Operations Report, and MODA Rebate Report and compares them to prior periods to ensure that trends are aligning with expectations and that the amounts reported by third-party administrators to Milliman are complete and accurate.

The understanding for this system is documented above in the "Controls - Actuarial Report" step.

### **1. Confirmation of Key Manual Control:**

# State of Washington

We received a copy of the Monthly Operations Report from March 2024, which was a PDF file that had multiple comments on it indicating review. We also reviewed the MODA rebate report, which was an excel file featuring rebate data from FY21-23 and we inspected a screenshot of HCA's weekly claims tracker workbook – both of these documents had rebate/claims data from FY21-23, denoting that current rebate/claim trends are being compared to prior periods to ensure trends align with expectations. **No issues noted.**

## **Noted Weaknesses are as follows:**

None.

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.1.PR.G - Claims and Judgments Payable**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* EZM, 5/6/2024

*Reviewed By:* RKM, 5/29/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To confirm HCA reviewed Milliman's incurred but not paid memo to ensure accuracy (Key Control #2 for Actuarial Report) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

# State of Washington

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.



# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control #2 (Valuation):** Milliman calculates and prepares the memo that summarizes the calculations for the incurred but not paid (IBNP) estimate in accordance with the data provided by Regence, MODA, Delta Dental and HCA, then meets with the ERB finance team to discuss the memo and compare it to prior quarters before the ERB Section Manager approves it.

The understanding for this system is documented above in the "Controls - Actuarial Report" step.

### **1. Confirmation of Key Manual Control:**

For the December 31, 2023 reserve, HCA was provided the finalized memo on January 31, 2024. The ERB Finance Team met with Milliman on January 12, 2024. We confirmed this meeting took place by inspecting a copy of the Weekly Milliman Call agenda for the same date. Milliman and the ERB Finance Team discussed the general trends observed in the reserve memo, differences from prior periods for both the PEBB and SEBB programs, and discussed general seasonality of claims trends. The ERB finance team approved the memo. **No issues noted.**

### **Noted Weaknesses are as follows:**

None.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **F.1.PR.G - Claims and Judgments Payable**

## State of Washington

*Procedure Step:* Key Control #3 (Manual)  
*Prepared By:* EZM, 5/2/2024  
*Reviewed By:* RKM, 5/6/2024

### Purpose/Conclusion:

#### **Purpose:**

To confirm the preparation and review of JV adjustments to the incurred but not paid liability (Key Control #3 for Actuarial Report) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude*

## State of Washington

*and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements.*

## State of Washington

*In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #3 (Valuation): Quarterly, a Fiscal Analyst 5 prepares the journal voucher based on the IBNR summary charts in the Milliman memo. The Deputy Accounting Section Manager reviews the journal vouchers to adjust the incurred but not reported liability to ensure the amount is supported by the memo from Milliman, HCA agrees with the conclusions and analysis in the memo, and the IBNR amount is correctly calculated.**

The understanding for this system is documented above in the "Controls - Actuarial Report" step.

### **1. Confirmation of Key Manual Control:**

We reviewed PAJV6033 which adjusted the PEBB IBNP liability. We reviewed the the JV cover sheet, Milliman's memo, and the excel workbook (PAJV6033-file0002-FY24 Q2-PEBB IBNR balances.xlsx) used to calculate the adjustment with account codes. The PEBB IBNP liability totaled \$142,763,000 as of December 31, 2023. We noted the JV was prepared by Kathy Plaquet, FA 5, on 2/5/2024. We noted Rita Homan, Deputy

# State of Washington

Accounting Section Manager, reviewed and approved PAJV6033. IBNP adjustments tied to the memo without exception.

We reviewed SAJV1441 which adjusted the SEBB IBNP liability. We reviewed the the JV cover sheet, Milliman's memo, and the excel workbook (SAJV1441-file0002-FY24Q2-SEBB IBNR balances.xlsx) used to calculate the adjustment with account codes. The IBNP liability totaled \$68,303,000 as of December 31, 2023. We noted the JV was prepared by Kathy Plaquet, FA 5, on 2/6/2024. We noted Rita Homan, Deputy Accounting Section Manager, reviewed and approved SAJV1441. IBNP adjustments tied to the memo without exception.

## Noted Weaknesses are as follows:

None.

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.1.PR.G - Claims and Judgments Payable**

*Procedure Step:* Rely on Specialist

*Prepared By:* EZM, 10/16/2024

*Reviewed By:* RKM, 10/17/2024

Purpose/Conclusion.\*

### **Purpose:**

To determine if we can rely on the work of HCA's external health care actuary, Milliman, to provide audit evidence for the Incurred But Not Paid (IBNP) liability (claims and judgments payable) estimate.

### **Conclusion:**

We determined that we **can** rely on the work of the specialist.

# State of Washington

## Testing Strategy:

To determine whether the audit can rely on the work of the outside specialist and whether the specialist's work supports the financial statements, the following procedures are **required** to be performed:

Auditor should check with their supervisor whenever they determine that the use of a specialist may be necessary.

*A specialist is an individual or organization possessing expertise in a field other than accounting or auditing (for example, information technology specialists, engineers and actuaries). Specialists may be contracted or employed by entity management to assist them in performing their responsibilities (management's specialist) or contracted or employed by our Office (auditor's specialist).*

*This step does not need to be completed when consulting with attorney general assistants, LGS, TAS, LISA, STAT, DSI or "Subject Matter Experts" designated on the intranet. Contact TAS for assistance if needed to determine whether someone would be considered a specialist or not.*

Assess the specialist's competence, capability and objectivity as it relates to the work that we intend to rely on for the audit.

*Competence refers to the specialist's relevant qualifications and experience. In assessing competence, auditors should consider:*

*The education, professional certifications or licenses of the specialist in his or her field, as appropriate.*

*The reputation and standing of the specialist.*

*The specialist's experience in the type of work under consideration.*

*Our Office's experience in using the specialist's work, if applicable.*

*Capability refers to effect of any access, resource or other limitations on the specialist's work. In assessing capability, auditors should consider:*

*Timing of the specialists work*

*Any significant limitations on the specialist's access to needed information or people*

*Any significant limitations on the time the specialist was able to devote to the work*

*Our Office's experience in using the specialist's work, if applicable.*

*Objectivity refers to the possible effects of any bias, conflicts of interest or undue influence on the specialist's judgment. If the*

## State of Washington

*specialist's objectivity is impaired, the auditor may not rely on the work of the specialist. In assessing objectivity, auditors should consider:*

*Any pressures or incentives on either specialists or management to misstate*

*Threats to objectivity of the specialist (including self-interest, advocacy, familiarity, self-review or intimidation threats) and any safeguards in place (segregation of duties, lines of reporting, professional standards, formality and consistency of methods and assumptions, retrospective reviews, etc)*

*Our Office's experience in using the specialist's work, if applicable.*

*Auditors should contact TAS if the auditor has any concerns with assessing the competence, capabilities or objectivity of specialists.*

Obtain an understanding of the work and conclusions of the specialist. This understanding should include the following elements:

- Objectives and scope of the specialist's work
- Intended use of the specialist's work to support the audit objective
- Specialist procedures and conclusions
- Assumptions and methods used by the specialist

*The objectives and scope of the specialists work and intended use of the specialist's work to support our audit objective should have already been included in the audit plan or else will need to be documented as a change to the audit plan.*

Evaluate the work and conclusions of the specialist. This evaluation should include the following elements as applicable:

Relevance and reasonableness of the specialist's methods and assumptions

*The appropriateness and reasonableness of methods and assumptions used and their application are the responsibility of the specialist. However, if the auditor concludes that the specialist's findings are unreasonable in the circumstances, the auditor should apply alternative procedures, which may include obtaining the opinion of another specialist.*

*Auditors should specifically consider whether methods and assumptions changed from the preceding period and the reasons for such changes, if applicable.*

Appropriate tests of source data provided by the entity to the specialist.

*If any data used by the specialist was provided by the entity, the auditor should consider the risk that incomplete or inaccurate data may materially affect the specialist's conclusions. This risk may be affected by the auditor's assessment of overall COSO elements*

## State of Washington

*and control risk for the related system.*

*For example: when relying on work of an actuary for self-insurance liabilities, auditors would normally verify the completeness and accuracy of claims information provided to the actuary against claims information per the pool's system. This can be done by comparing the total claim payments per pool's records to total claims paid shown on the actuary reports (in aggregate or on annual basis) – the figures may not match exactly but should be very close.*

Relevance and reasonableness of the specialist's conclusions.

Verifying that the specialist's conclusions are reflected in the financial statements

Add an additional representation to the rep letter if the specialist used was employed or contracted by management (rather than SAO). See the List of Additional Representations located in the Auditor Reference Guide here: [Representation Letter Resource.docx](#)

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [3230](#) - Using the Work of Specialists**

Record of Work Done.:

### **Assessment of Competence, Capabilities and Objectivity of Specialist**

We assessed the competence, capabilities and objectivity of the specialist, specifically considering factors described in the testing strategy.

#### *Competence*

To determine competence, we considered:

*The education, professional certifications or licenses of the specialist in his or her field, as appropriate.*

*The reputation and standing of the specialist.*

*The specialist's experience in the type of work under consideration.*

*Our Office's experience in using the specialist's work, if applicable.*

**Aaron Gates, FSA, MAAA**

**Milliman Consulting Actuary**

Mr. Gates was based in Milliman's Seattle, Washington office and he joined the firm in 2011. He was listed on Milliman's web site, see bio link



## State of Washington

[here](#). Mr. Gates graduated with a bachelor of science in mathematics in 2009.

We confirmed Mr. Gates's FSA and MAAA credentials by reviewing the actuary directory on the Society of Actuaries (SOA) website (<https://www.soa.org/>). We noted he received his MAAA in 2013 and his FSA in 2016. We noted he was also listed as compliant (2020-2021 and 2021-2022) for Society of Actuaries continuing professional development (SOA CPD) attestation. These were the most recent CPD cycles. We also noted his listed primary area of practice and specializations were consulting and health. Based on review of Mr. Gate's credentials, we determined Mr. Gates was a competent specialist.

### **Jordan Pettibon, FSA, MAAA** **Associate Actuary**

Mr. Pettibon was based in Milliman's Seattle, Washington office and he joined the firm in 2014. He was listed on Milliman's web site, see bio link [here](#). Mr. Pettibon graduated with a B.A. in Mathematics, and a B.S. in Economics in 2014.

We confirmed Mr. Pettibon's FSA and MAAA credentials by reviewing the actuary directory on the Society of Actuaries (SOA) website (<https://www.soa.org/>). We noted he received his MAAA in 2017 and his FSA in 2021. We also noted he was also listed as compliant (2021-2022 and 2022-2023) for Society of Actuaries continuing professional development (SOA CPD) attestation. These were the most recent CPD cycles. We also noted his listed primary area of practice and specializations were consulting, health and health insurance - commercial. Based on review of Mr. Pettibon's credentials, we determined Mr. Gates was a competent specialist.

As HCA's contracted external health actuary, SAO has years of experience with Milliman. This includes the calculation of the key figure of Transactions Subsequent to the Measurement Date as part of the State's OPEB Schedules. We performed an additional review of Milliman's competence as part of [S1FinancialManagement-FS24]. Based on our Office's experience with Milliman we determined Milliman was a competent specialist.

### *Capability*

To determine capability, we considered:

*Timing of the specialists work*

*Any significant limitations on the specialist's access to needed information or people*

*Any significant limitations on the time the specialist was able to devote to the work*

*Our Office's experience in using the specialist's work, if applicable.*

Milliman is contracted with HCA to perform actuary services for HCA. Milliman is in weekly contact with HCA, primarily the ERB finance department. Sara Whitley, HCA ERB Finance Manager, worked with Milliman regularly. She participated in regular reviews of Milliman's work and deliverables. We inquired with Sara regarding any non-compliance with any deliverables, and she was not aware of any. Services were on-going and had deliverables related to the following through a biennium:

## State of Washington

Generation of financial statement estimates made quarterly (incurred but not paid liability, premium stabilization reserves, restricted fund amounts, etc.),  
Financial record keeping for PEBB operations (historical claim costs for all plans offered),  
Future projections and other budgetary information used by HCA, OFM, the Governor's Office, and the legislature,  
Assisted with determination of premiums for employees, retirees, and other index rates (state agency employer contributions)  
Information shared with various unions and collective bargaining units.

Milliman obtains claim data for all PEBB and SEBB plans on a regular (daily, weekly, and monthly) basis directly from the following providers (used in IBNR reserve estimates):

Regence (claims processor for all Uniform Medical Plans, HCA's self-insurance health care plan family)  
MODA (pharmacy claims processor, HCA's self-insurance health care plan family)  
Kaiser Permanente Northwest  
Kaiser Permanente Washington  
Premera Blue Cross  
United Healthcare  
Delta Dental (claims processor for Uniform Dental Plan or UDP, HCA's self-insurance dental care plan)

Used for other purposes:

Davis Vision  
EyeMed Vision Care  
MetLife  
Delta Care  
Willamette Dental Group

For the IBNR estimate specifically, Milliman follows the industry standard of quarterly IBNR estimates, which helps ensure accurate financial reporting and effective risk management. Based on Milliman's relationship with HCA, direct access to claims data, reasonable performance on all contract deliverables, and our experience with Milliman, we determined Milliman was a capable specialist.

### *Objectivity*

To determine objectivity, we considered:

*Any pressures or incentives on either specialists or management to misstate*

*Threats to objectivity of the specialist (including self-interest, advocacy, familiarity, self-review or intimidation threats) and any safeguards in place (segregation of duties, lines of reporting, professional standards, formality and consistency of methods and assumptions, retrospective reviews, etc)*

*Our Office's experience in using the specialist's work, if applicable.*

## State of Washington

We noted Milliman was a nation-wide actuary firm and leader in employee benefits, pensions, and health care. Milliman was not financially dependent on revenue generated from the Health Care Authority. During our 2024 control meetings, we inquired regarding the relationship between HCA and Milliman. HCA did not disclose any objectivity concerns. We noted HCA contracted with Milliman for professional services (actuary and consulting services) since 2007 (contract awarded in 2006). We considered objectivity risks, specifically risks related to familiarity and self-review. Due to the length of HCA's and Milliman's relationship, the evolution of health care, and reliance on financial tools developed by Milliman, we inquired about safeguards. Per Sara Whitley, ERB Finance Manager, Milliman maintains a strict review policy, where all deliverables and analyses are reviewed by actuaries outside of the Seattle Health practice. Beyond the standard Milliman peer review process internal to each practice, external review requires that they have the deliverables reviewed by a principle from another practice that is financially independent from Seattle Health. Finally, Milliman also produces retroactive reserve estimates so that both Milliman and HCA may be aware of any consistent bias in their estimates (i.e. whether they consistently overestimate, underestimate, or have a mix of both). **Auditor Note:** We did not meet directly with Milliman, as we would be charged an hourly fee.

Milliman uses nation-wide health care trends in their models to ensure results produced relevant information that was not financially skewed (i.e. future health care costs did not exceed national GDP, future costs were capped at a percent of national GDP, nation wide trends prevented skewed regional data). We noted Milliman used their internally developed national trends. We reviewed descriptions of Milliman's Health Cost Guidelines (HCG) on their website at <https://us.milliman.com/en/products/hcgsuite>. National trends included the following products: Ages 65 and Over, Commercial, Dental, Grouper, Prescription Drug Rating Manual, and Reinsurance.

Based on our experience, inquiry, and review of assumptions, we determined Milliman was an objective as a specialist.

### **Understanding of Specialist's Work and Conclusions**

We gained an understanding of the specialist's procedures and conclusions, including the methods and assumptions used, and noted the following:

Milliman was HCA's external actuary and health care consultants. Milliman prepared the incurred but not paid (IBNP) memo as one of many deliverables and services provided to HCA to manage their self-insurance plans offered under the Uniform Medical Plan group. Milliman obtained claims data directly from Regence, MODA and Delta Dental, HCA's third party administrators for claims processing. HCA provided Milliman AFRS data. AFRS data was provided by Rita Homan, HCA Assistant Accounting Section Manager, and Sara Whitley, HCA ERB Financial and Data Analyst. The IBNP report was used by Rita Homan to prepare and support journal vouchers to quarterly adjust AFRS.

We reviewed the forecast memo that described the general assumptions and methodologies used by Milliman for both PEBB and SEBB. See [\[Milliman Trend Model\]](#). Milliman noted specific assumption and methodology adjustments in the IBNP memo. The IBNP estimate was based on historic and projected trends in claims. SAO determined that Milliman's assumptions and methodologies were reasonable and produced a reasonable IBNP estimate. Based on SAO's understanding, Milliman's work included all self-insurance plans operated by HCA (PEBB and SEBB) and

## State of Washington

reflected the benefits offered. **No issues noted.**

### **Evaluation of Specialist's Work**

See Milliman's incurred but not paid (IBNP) estimate for June 30, 2024 at [[PEBB and SEBB Reserve Analysis - June 30 2024 Reserve Adjustments](#)]. We also reviewed the assumptions and methodology used by Milliman at [[Milliman Trend Model](#)]. We tested the consistency of the report and source data used at [[Claims and Judgements Payable Testing](#)].

We inquired with Sara Whitley, HCA ERB Finance Unit Manager, about their processes for evaluating source data provided to the specialist and Milliman's work and conclusions. She noted the following:

As the sponsor and employer for the plans, HIPPA compliance rules limit the amount of access HCA has to the raw claims feed from the third-party administrators. As such, HCA relies on Milliman to complete the necessary analytical checks and balances on the raw data feeds to complete their analysis.

HCA (Specifically the Employee Retiree Benefits unit) and Milliman have a "Weekly Milliman Check-in" meeting that includes a discussion and review of Milliman deliverables, discussion of general program management topics, etc. At these meetings, Milliman will generally review documents with HCA ERB and the underlying conclusions, including the IBNR adjustment memo.

Following these meetings, ERB then reads and reviews the memos for reasonableness, compares the final calculations to previous interim analyses and follows up on any changes.

HCA does perform a review of the memo for general misrepresentations of information, reasonableness and ensures the underlying results are to be expected given their understanding of the data and detailed description of methodology.

HCA does have other tools and reports available that allow for comparisons to be made between Milliman's raw data and the information used to complete the IBNR memo each quarter. Some of these tools are:

Weekly lump-sum claims invoicing amounts - Generated internally based on invoiced amounts provided by Regence

Regency Monthly Operations Report - Provided by Regence

MODA Rebate Reporting - Provided by MODA

HCA uses these reports and compares them to prior periods to ensure that claims trends are aligning with expectations. HCA has limited access to raw claims feed data due to HIPPA compliance rules as the plan sponsor and employer.

We performed the following tests:

Tied the IBNP liability to the financial statements/general ledger [See tab "Step 1" here: [Claims and Judgements Payable Testing](#)] to ensure Milliman's conclusion were reflected in the financial statements (Valuation).

Tied the summary IBNP liability from the summary tables [See tab "Step 2" here: [Claims and Judgements Payable Testing](#)] presented in the narrative to the detailed attachments that presented IBNP liabilities by plan. This step was performed to ensure Milliman's conclusions were consistent throughout the memo which was an exception from the FY21 ACFR.

Tied claim data reported in lag tables to the general ledger [See tab "Step 3" here: [Claims and Judgements Payable Testing](#)] to ensure accurate and complete source data was provided to Milliman.

## State of Washington

SAO noted the following results from our tests:

We tied the IBNP reported in Milliman's memo to the leadsheet and financial statements. **No issues noted.**

We tied the summary IBNP estimate to the supporting attachments which listed the IBNP by plan and by significant claim type (medical, pharmacy, and dental). Amounts tied within rounding. **No issues noted.**

We tied self-insurance claim expenses (Premiums and Claims) from AFRS to the lag tables in Attachment 15 by plan and significant claim type. **No issues noted.**

Based on our test results and other procedures performed above, SAO determined we could rely on Milliman's work and that Milliman's conclusions were relevant and reasonable. **No issues noted.**

We will include the following additional representation as part of the management representation letter [[FS Letter of Representation](#)]:

We adequately considered the qualifications of Milliman and agree with conclusions regarding:

Health Insurance Fund - Claims and Judgments Payable

### F.1.PRG - Claims and Judgments Payable

*Procedure Step:* Risk Assessment

*Prepared By:* EZM, 5/17/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion.:

#### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy.:

Auditors are **required** to perform the following procedures for each line item:

#### **STEP 1: Inherent Risk (IR)**

## State of Washington

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if

## State of Washington

setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation – **HIGH**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

Actuarial Report (Valuation) –

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation – **HIGH**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:



## State of Washington

We will complete the testing strategy for relying on the work of specialists [Rely on Specialist] to ensure the actuary was competent. Standard procedures include assessing the competency of Milliman, obtaining and reviewing the data used by the actuary, reviewing assumptions, and concluding on the work performed by specialists. We will obtain the FY24 Q4 Milliman reserve memo. We will tie tables in the reserve memo's narrative to detailed exhibits by plan (triangle tables). We will also tie the claims in the detailed exhibits by plan to the claims expenses in AFRS, within reason.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### F.1.PRG - Claims and Judgments Payable

*Procedure Step:* Substantive Test

*Prepared By:* EZM, 10/11/2024

*Reviewed By:* RKM, 10/16/2024

Purpose/Conclusion.\*

#### **Purpose:**

To determine whether current liabilities were reported at properly valued or calculated amounts.

#### **Conclusion:**

We determined that current liabilities were reported at properly valued or calculated amounts. **No issues noted.**

Testing Strategy.\*

The following is a list of **considerations** for testing the valuation assertion for current liabilities. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

*For current portions of long-term liabilities*, see the valuation testing strategy for non-current liabilities. The same strategies can be applied to the entire liability, covering both current and non-current portions.

Recalculate or review entity calculations of accruals (such as withholding taxes, accrued payroll, payroll taxes, accrued interest payable, etc).

## State of Washington

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Certificate of Participation (COP) Confirmations** (*applies to state agencies, including community colleges and universities*) - listing of outstanding COP debt at fiscal year end obtained directly from the State Treasurer

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS 3.4.1 Leases** - includes accounting procedures applicable to municipal leases

**BARS 3.4.4 Refunding Debt**

**BARS 3.4.9 Risk Management Principles**

**BARS 3.4.15 Legal and Other Contingencies**

Record of Work Done:

### **Substantive tests performed to meet the Valuation assertion:**

We completed the testing strategy for relying on the work of specialists [Rely on Specialist] to ensure the actuary was competent. We followed standard procedures including assessing the competency of Milliman, obtain/review data used by the actuary, review assumptions, and conclude on the work performed by specialists. We tied the tables in the reserve memo's narrative to detailed attachments by plan (lag triangle tables) and tied the claims in the detailed attachments by plan to the claims expenses in AFRS, within reason.

Testing Results: [Claims and Judgements Payable Testing]. We tested this balance for the valuation assertion and we determined that the balance was properly valued. **No issues noted.**

### **F.2.PR.G - Premiums and Assessments**

# State of Washington

*Procedure Step:* Summary & Conclusion

*Prepared By:* MRF, 10/3/2024

*Reviewed By:* RKM, 11/26/2024

Purpose/Conclusion.

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy.

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

# State of Washington

## Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

**(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined the results of substantive tests do not indicate a need to modify our risk assessment.

**(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We determined the quality and quantity of evidence obtained was sufficient and appropriate.

## **F.2.PRG - Premiums and Assessments**

*Procedure Step:* Understanding of Line Item

*Prepared By:* MRF, 5/22/2024

*Reviewed By:* RKM, 5/29/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

# State of Washington

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

## **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

## **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is*

## State of Washington

*understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

**(1) Prior Audit Exceptions:**

We noted **no** prior audit exceptions.

**(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

This line item primarily consists of premiums collected for medical insurance, dental insurance, and other insurances (i.e. life, long-term disability, etc.). HCA collects premiums for both purchased and self-insurance premiums, most of which are from participating employers. The amount participating employers pay is the employer premium (the State Index Rate for most employers) and the premiums withheld from employees through payroll deductions. Most state agencies pay through account transfers and non-state agencies remit payments to a lock box. COBRA and other self-pay subscribers remit payments to a lock box service. HCA uses an individual lock box for each fund to ensure payments are accurately reported.

Pay1 calculates and prepares monthly bills for participating employers. Invoices are delivered as follows:

HRMS employers - delivered via paper print out or EOS report distribution system (electronic) which is automated by the Pay1 IT team

K-12 actives, Political Sub-Divisions - printed and delivered via US mail, or electronically through MFT if electronic delivery is requested by the employer. The MFT registration is managed by the Pay1 IT team.

*ACFR Database*

We analyzed the revenue amounts in the line item lead sheet and identified funds 493 (School Employees' Insurance Account) and 721 (Public Employees' and Retirees Insurance Account) as the significant funds for this line item.

We identified no unusual or unexpected elements, amounts, or changes that may indicate risk.

**(3) Updates to Significant Account Matrix:**

None.

# State of Washington

## F.2.PR.G - Premiums and Assessments

*Procedure Step:* Controls - Pay1  
*Prepared By:* MRF, 5/16/2024  
*Reviewed By:* RKM, 9/11/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:



## State of Washington

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to

## State of Washington

just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls in the Pay1 system address the following balance(s):

Health Insurance - Premiums and Assessments

Business-Type Activities - Charges for Services: Health Insurance

For the following assertions:

# State of Washington

Occurrence - There is a risk that recorded revenue is more than source records.

Valuation - There is a risk that insurance premiums (employer and employee) for the various plans were not calculated correctly by Pay1.

## **Gain an Understanding of Internal Controls**

See Health Insurance Activities [[Health Insurance Activities Updated 2024](#)] for the following:

How contribution rates were established for PEBB and SEBB (required premiums from employers or all eligible employees regardless of the employee's participation in PEBB or SEBB)

Rate factors for subscribers and the different dependents they could enroll.

Surcharges (i.e. tobacco surcharge)

Listing of insurance products offered for plan (calendar) year 2023 and 2024

Eligibility requirements for PEBB and SEBB

Key information maintained in Pay1

We met with the following HCA staff on 05/07/2024 to gain an understanding of internal controls relating to Pay1:

Rita Homan, Deputy Accounting Section Manager

Lisa Kolle, PEB Accounting Manager

William Sogge, Audit Liaison

Pay1 maintains key information for all subscribers and dependents. Participating employers are responsible for accuracy of demographic information and elections maintained in Pay1. Based on current month elections entered or imported into Pay1 by the participating employer and rate tables maintained in Pay1, Pay1 automatically calculates the amount due for each individual subscriber in an itemized monthly bill by SSN (**Key Control #1 - Automated Software Calculation - Valuation and Occurrence**). The subscriber premiums are added to the employer premiums to calculate the total amount owed to HCA per subscriber. The employer premiums are determined by the State Index Rate, or for Political Sub-Divisions, a contracted rate. The State Index Rate is determined semi-annually by the Legislature.

Currently, Political Sub-Divisions are the only participating employers that do not pay the state index rate. HCA bills these groups monthly based on a contracted rate. The amount the employers pay is dependent on the number of subscribers they have enrolled, and it is the employer's responsibility to determine and maintain subscriber eligibility. Invoices are reviewed by a Contract Manager, an HCA employee that specializes in specific contracts with participating employers, for reasonableness.

Bills are prepared for each participating employer on the following cycles:

23rd of each month - self-pays (i.e. COBRA subscribers, self-pay, retirees not paid with DRS deductions, and K-12)

26th of each month - all other employer groups, retirees with DRS deductions, higher education

Last day of each month - state agencies that used HRMS

## State of Washington

Note: Bills are prepared and remitted prior to the month of service. HCA expects participating employers to reconcile their respective bills to ensure accuracy of listed subscribers.

HCA prepares participating employers' invoices prior to the month of service. To ensure that billings existed, Pay1 reflected each respective agency's subscribers, and that Pay1 accurately exported activity to AFRS, HCA relies on matching payments with invoices. Payments come via lockbox from US Bank and are automatically processed by Pay1 unless an error occurs. ERB accountants review lockbox reports daily, and match payments for completeness and accuracy. The ERB accountants monitor revenues and cash receipts to ensure bills prepared by Pay1 are accurate and match the amounts in AFRS. If the amount in AFRS does not match the amount collected in Pay1, an In-Process Report is automatically generated. This report provides details on any discrepancies between the amount in AFRS to the amount in Pay1. The ERB Accountants review this report daily, and address any discrepancies (**Key Control #2 - Manual - Occurrence**).

### **Adjusting Entries - Prepayments/Credit Balances**

At the end of the month, Pay1 automatically generated aging reports based on customer type. Pay1 generated the following reports:

- bh#grp.txt
- bh#ind.txt
- pebb#grp.txt
- pebb#ind.txt, PAY1 report HRISD-B5519-R01
- sebb#ind.txt, Pay1 report SEBB-B5519-R01
- excrpt.txt

Monthly, IT generates printed receivable reports from Pay1 titled HRISD-B5519-R01 and SEBB-B5519-R01. ERB Fiscal Analyst 4s review reports for reasonableness and convert the reports to Excel for retention purposes. These reports summarize all receivables and unearned revenue (pre-paid) for each group (Self-Pay Agencies, K-12 Agencies, Retirees, etc.). Rita Homan, Assistant Accounting Section Manager, reviews the reports manually at the end of every month to ensure the reports are free of errors.

FA4's use the HRISD-B5519-R01 and the SEBB-B5519-R01 reports to prepare backup for unearned revenue journal vouchers. The FA4 uses the Excel workbook to prepare the journal vouchers to post prepaid receivables to unearned revenue. FA5s, ERB Accounting Manager, or the Assistant Accounting Section Manager will review the JVs and aging reports to ensure the unearned revenue balances were accurate and represented actual amounts from Pay1 prior to posting (**Key Control #3 – Manual – Valuation**).

### **How Transactions are Recorded in AFRS:**

Pay1 automatically posts transactions to AFRS in a nightly batch. General ledger balances are reviewed in detail for reasonableness by a FA5, Assistant Accounting Section Manager, or ERB Accounting Section Manager when ERB prepares the quarterly financial statements.

# State of Washington

## Key Controls are as Follows:

Key Control #1 (Automated Software Calculation) - Valuation & Occurrence: Pay1 automatically calculates and prepares monthly billings based on current month subscriber elections maintained in Pay1. Pay1 automatically prepares billings based on approved employer and employee rates.

Key Control #2 (Manual) - Occurrence: Daily, ERB accountants review payments automatically processed and not automatically processed, in Pay1, and reconcile payments to AFRS to ensure that revenues/receivables occurred and are accurately classified in the Pay1 System.

Key Control #3 (Manual) - Valuation: Monthly, ERB FA4s manually record unearned revenue (and receivables) related to PEBB/SEBB premiums by journal voucher. Entries to record unearned revenue (and receivables) are based on Pay1 aging reports HRISD-B5519-R01 and SEBB-B5519-R01. The entry is reviewed by the FA5, ERB Accounting Section Manager, or Deputy Accounting Section Manager to ensure accuracy of entries.

## Noted Weaknesses are as Follows:

None

## F.2.PRG - Premiums and Assessments

*Procedure Step:* Key Control #1 (Automated)

*Prepared By:* MRF, 5/22/2024

*Reviewed By:* RKM, 6/5/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To determine whether Pay1 automatically calculates and prepares monthly billings based on current month subscriber elections maintained in Pay1 and prepares billings based on approved employer and employee rates (**Key Control #1 for Pay1**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

# State of Washington

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation: This is the one for the control- Need ERB finance team for information?**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

Deleted other sections for clarity.

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, **consider** the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

## State of Washington

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

**"What is the single most important General IT control related to this calculation?"**

Like they make a change annually with rate tables, what is the verification process? Who performs what review, when, and how is it documented?

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

## State of Washington

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.



## State of Washington

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period. If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel. If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Information Technology](#) Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

#### Manual vs. Automated Interfaces

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

## State of Washington

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program,

## State of Washington

also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An "**electronic signature**" can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A "**digital signature**" is a legal signature with a formal certification process that documents who approved the document and ensures the

## State of Washington

document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

### **Premiums and Assessments- Valuation and Occurrence**

**Key Control #1 - Automated Software Calculation** - Pay1 automatically calculates and prepares monthly billings based on current month subscriber elections maintained in Pay1. Pay1 automatically prepares billings based on approved employer and employee rates.

### **STEP 1: Understand Automated Key Control**

The understanding for this key control is documented above in the "Controls - Pay1" step.

### **STEP 2: Confirm and Test Automated Key Control:**

We received a walk through by Rita Homan, Deputy Accounting Section Manager, for the recalculation for selected transactions on May 7, 2024.

We selected four categories and then selected an individual for recalculation of their monthly billing:

- Regular PEBB state agency - DSHS
- SEBB - School employee at agency 600 H01
- Political sub-division/group - Olympic Medical Center
- Retiree, no specific employer

For each, we reviewed the Pay 1 system for elections and total, compared the published rate tables on HCAs website, and compared the totals to the billing invoice generated in Pay1.

## State of Washington

### PEBB (DSHS)

We recalculated the elections made by employee XXX-XX-1826 for May 2024. We did this by taking the PEBB base employer premium of \$1,145 from the [HCA website](#) and adding the employee premium based on their election. Their election included the \$124 basic rate for Uniform Medical Plan (UMP) which ties to the rate tables published, with a \$25 tobacco surcharge for a total election of \$149, for a total of \$1,294. We noted their "HSA Family Comp" in Pay1 was listed as "1" meaning only the subject was covered, with no spouse or children on the plan. Premium tied without exception between billing statement, pay1, and rate tables. We also noted the May coverage period was invoiced on April 25, 2024. **No issues noted.**

### SEBB

We recalculated the elections made by employee XXX-XX-2091 for May 2024. We noted their Pay1 elections listed "PH" as their health carrier, which is Premera Blue Cross High PPO, and their "HSA Family Comp" was "4" meaning it was the subscriber, spouse, and at least one child, which is also categorized as "full family" in the rate tables. Per the rate tables on the [HCA website](#), the employer premium is \$1,100 and the employee premium was \$345, which matched the amount billed in Pay 1, for a total billed invoice of \$1,445. Premium tied without exception. We also noted the May coverage period was invoiced on April 15, 2024. **No issues noted.**

### PEBB Political SubDivision (Olympia Medical Center)

We tied the elections made by employee XXX-XX-0448 for May 2024 to the premium charts on the [HCA website](#). We noted the Pay1 elections listed Carrier U for coverage which is Uniform Medical Basic, and their "HSA Family Comp" was "4" meaning it was the subscriber, spouse, and at least one child, which is also categorized as "full family" in the rate tables. We tied the UMP classic full family tiered rate listed on the website, the amount billed which was \$2,428 with a \$33 surcharge. We noted the May coverage was billed on April 26, 2024. **No issues noted.**

### Retiree

We recalculated the elections made by self-pay employee XXX-XX-7641 for May 2024. We reviewed the Pay1 screen and noted their elections were for carrier "F" which is Medicare Plan F, and they elected to have dental. Their "HSA Family Comp" was "1" meaning only the subscriber was covered. We compared this information to the rate tables on the [HCA website](#) where we tied medical to \$119 and dental to \$49, for a total billing amount of \$168. We tied this to the billed premium which was invoiced on April 23, 2024. **No issues noted.**

### **Noted Weaknesses are as follows:**

None

### **STEP 3: Understand General IT Controls**

We met with the following HCA staff on 05/15/2024 to gain an understanding of general controls for the automated calculation performed by Pay1:

Grant Stromsdorfer, Pay1 mainframe IT developer

# State of Washington

Sara Whitley, Employee Benefits Board (ERB) finance manager

Rates are updated throughout the year depending on the coverage type. PEBB and SEBB rate premiums update on an annual basis in June/July, state share rates in May, and composite rates update in September. Each year, the finance team reaches out to the carriers in the "request for renewal" cycle. Each carrier that would like to continue must provide updated rates to HCA. HCA requires these rates to be "actuarially sound" and signed off by an actuary. Milliman performs this service for Uniform Medical Plan (UMP) classic. Once each carrier has submitted their new premium rates to ERB, ERB compiles the information into a large excel file named the "rate book". The rate book is presented to the appropriate board (Public Employees Benefits Board, or School Employee Benefits Board) for adoption.

After approval, the rate book is submitted to the Pay1 mainframe IT team via email. This email triggers a help desk ticket that pulls the IT team into the workflow and all correspondence is maintained within the email thread to ensure all details and actions are recorded. A Pay1 contractor will update the rates in a Pay1 test environment. Only the Pay1 contractors have the ability to update the information, the HCA IT team is responsible only for testing the new information.

Grant Stromsdorfer, Pay1 Mainframe IT Developer, then pulls the rate information out of the test environment as a txt file and converts it back into an excel workbook. He reviews the newly generated rate tables, to the tables submitted by the ERB team to confirm the data has been correctly entered. He also performs summation tests to confirm the new totals match. Each type of coverage, medical, dental, vision, etc. gets reviewed in its own tab. If everything is correct, he sends his excel workbook via email with any notes to Tanya Deuel, ERB Finance Manager, for secondary review to ensure updates are correct (**General IT Control #1**).

After the ERB Finance Manager confirms the information is correct, the HCA IT team will set a release date for the updated rate tables from the testing environment, to go into live production. As HCA is not aware of any instances of post verification software corruption that occurs between the test environment, and live status, they do not run an additional check in the live environment.

## **STEP 4: Confirm Key General IT Controls**

**General IT Control #1 (Manual) - Valuation:** The HCA Pay1 mainframe IT team reviews the updated rate tables pulled from a Pay1 testing environment and compares rates and totals to the original tables submitted by the ERB team. If updates have loaded correctly, Pay1 mainframe employees send a notification of review and their workpaper back to the ERB Finance Manager for secondary review to ensure updates are correct, before the updates are released into production.

We received a walk through of the rate table update for PEBB composite state shares by Grant Stromsdorfer, Pay1 Mainframe IT Developer, on May 15, 2024.

Grant walked us through the email thread detailing the conversations between Pay1 contractors, HCA IT staff, and the ERB finance team. We noted on May 3, 2024, Joselito Almazora (Pay1 Contractor) sent an email to his team, and cc'd Grant, which noted the had uploaded the 2024 PEBB State Share rate, and attached relevant text files such as

## State of Washington

"N:\IS\Operations\PEBB\Pay1\Mainframe\INSURANC\RATES\StateShare\2024StateShare\PEBB\_2024\_Health\_State\_Share.txt"

Grant then walked us through the original ERB submitted workbook "2024 PEBB Composite Rate Book", the txt file where the data is converted into a Pay1 usable format, and his resulting converted excel workbook "PEBB FY 25 State Share gs review 20240506.xlsx". We noted the review workbook had multiple tabs, one for each type of coverage, and columns for the carrier codes, tobacco surcharge, and other coverage information. For ease of comparison to the original book, Grant had added additional columns which included the carrier names, the coverage description, and additional notes such as political subdivision. Grant demonstrated that the columns in green were the reviewed information and included the employer premiums for higher education (HIED), general education (EMP K12), and political subdivisions (POL SUB). We also noted the effective date column for each of these changes was listed as 07/01/2024, which is when the new rates will be effective. We traced the rate for Kaiser Permanente NW classic (effective 07/01/2024 through 06/30/2025) from the original ERB rate book, into the text file, and the review workbook. We noted the effective date (07/01/2024), carrier premium (\$1,040) subscriber share (\$226), tobacco (\$25), and spouse surcharge (\$50) all tied with no variance.

We then reviewed the email chain, and confirmed the "PEBB FY 25 State Share gs review 20240506.xlsx" workbook had been sent to Tanya Deuel, ERB Finance Manager, on May 6, 2024 with a note stating it was ready for review. **No issues noted.**

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **F.2.PRG - Premiums and Assessments**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* MRF, 5/16/2024

*Reviewed By:* RKM, 5/29/2024

Purpose/Conclusion:
---------------------

#### **Purpose:**

To confirm ERB Accountants are reviewing payments automatically processed, and not automatically processed, in Pay1 and reconciling payments to AFRS to ensure the revenues occurred each day (key control #2 for Pay 1), in order to assess control risk.



# State of Washington

## **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

## State of Washington

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

# State of Washington

Guidance/Criteria:

Record of Work Done:

**Key Control #2 (Occurrence) Daily, ERB accountants review payments automatically processed, and not automatically processed, in Pay1, and reconcile payments to AFRS to ensure that revenues/receivables occurred and are accurately classified in the Pay1 System.**

The understanding for this system is documented above in the "Controls - Pay1" step.

## **1. Confirmation of Key Manual Control:**

We received a walk through from Rita Homan, Deputy Accounting Section Manager, on 05/01/2024. We received the lockbox reports, US Bank statements, TMS report, and the A7-A (Cash receipting JV) for the automatic lockbox report from HCA, for revenue received on April 10, 2024. We noted a total of \$2,640,203.69 was automatically processed in Pay1 from the following sources:

- PEBB E-Lockbox - Fund 721- \$89,442.06
- SD Benefits (box #94194) - Fund 493- \$1,971,398.00
- SEBB Retail (box #94115) - Fund 493- \$26,017.42
- Flex Spend (box #84245) - Fund 802- \$77,307.37
- Political Sub (box #84265) - Fund 721- \$256,076.92
- PEBB Retail (box #34270) - Fund 721- \$219,961.92

We noted the total of these payments tied to the total amount processed, \$2,640,203.69, with no exceptions. Additionally, we reviewed bank statements from US Bank and screenshots of Pay1 for each of the revenue sources above and confirmed the amounts tied with no exceptions. We also reviewed email correspondence of approval to upload the batch to TMS on April 11, 2024. The email correspondence of approval included several attachments such as a PDF report of the Lockbox amount and a screenshot of the cash receipts journal summary prepared by Diana Dunn, Medical Assistant Specialist 3, in the ProviderOne (Pay1) Accounting Unit.

We also reviewed the Pay1 reports for each of the lock boxes, and confirmed that all inputs were marked "Y" under valid. This indicates that all individual deposits being rolled into the lockbox total, had accurate information for automatic processing. Any deposit with a "N" would indicate the need for a manual review by staff before determining how to deposit.

We noted the Cash Receipts Journal Summary broke the amounts apart by fund to ensure funds were deposited correctly and the reconciliation was sent to Jennifer Adamire, Fiscal Technician 2. Jennifer then prepared the Batch for processing using the A7-A (Current Doc Number PACR4066), which was also approved on 04/11/2024 by Lisa Kolle, PEB Accounting Manager, and ties without issue to the amount processed.

# State of Washington

None of this revenue was manually processed in the Pay1 system. **No issues noted.**

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.2.PRG - Premiums and Assessments**

*Procedure Step:* Key Control #3 (Manual)

*Prepared By:* MRF, 5/16/2024

*Reviewed By:* RKM, 6/5/2024

Purpose/Conclusion.\*

### **Purpose:**

To confirm that monthly, ERB FA4s manually record unearned revenue (and receivables) related to PEBB/SEBB premiums by journal voucher, which is reviewed by the FA5, ERB Accounting Section Manager, or Deputy Accounting Section Manager to ensure accuracy of entries (key control 3 for Pay 1) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## State of Washington

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria.7
---------------------

# State of Washington

## Record of Work Done:

**Key Control #3 (Valuation):** Monthly, ERB FA4s manually record unearned revenue (and receivables) related to PEBB/SEBB premiums by journal voucher. Entries to record unearned revenue (and receivables) are based on Pay1 aging reports HRISD-B5519-R01 and SEBB-B5519-R01. The entry is reviewed by the FA5, ERB Accounting Section Manager, or Deputy Accounting Section Manager to ensure accuracy of entries.

The understanding for this system is documented above in the "Controls - Pay 1" step.

### **1. Confirmation of Key Manual Control:**

We obtained the March 2024 month end receivable adjusting journal vouchers from Rita Homan, Deputy Accounting Section Manager, for PEBB and SEBB. We received a walkthrough of the process on 05/01/2024 with Rita Homan.

#### **PEBB**

We obtained and reviewed the following JV:

PAJV6157 - To record PEBB unearned revenue for self-pay, prepaid receivables for revenue sources 000020 and 000021 per aging report dated 03/29/2024

We obtained the preparer/approver reporting from HCA IT for the selected JVs. The journal voucher was processed 04/02/2024, prepared by Michael Williamson, Fiscal Analyst 4, and reviewed by Brooke Schofield, Fiscal Analyst 5. The total amount posted was \$1,551,682.

We reviewed the monthly group aging report summary HRISDB5519-R01 with run date 03/29/2024. We noted prepaid amounts for Selfpay agencies was \$725,453 and amounts for retirees totaled \$30,388, for a total of \$725,453. We then reviewed the Summary Report for the JV and noted Revenue for Fund 107 000020 was \$632,433 and fund 107 000021 was \$93,020. These two revenue sources together ties to the \$725,453 determined in the aging report with no variance, and is included in the totals on the adjusting JV. Amounts posted in PAJV6157 tie without exception to Pay1 reports. **No issues noted.**

#### **SEBB**

We obtained and reviewed the following JV:

SAJV1477 - To record SEBB unearned revenue for self-pay, prepaid receivables for revenue source 000021 per aging report dated 03/31/2024

The journal voucher was processed 04/01/2024, prepared by Oanh Pham, Fiscal Analyst 4, and reviewed by Brooke Schofield, Fiscal Analyst 5. The total amount posted was \$145,853.

We reviewed the monthly group aging report summary SEBB-B5519-R01 with run date 03/29/2021. We noted prepaid amounts for Selfpay agencies was \$72,926. Amounts posted in SAJV1477 tie without exception to Pay1 reports. **No issues noted.**

**Noted Weaknesses are as follows:**

# State of Washington

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.2.PR.G - Premiums and Assessments**

*Procedure Step:* Risk Assessment

*Prepared By:* MRF, 10/22/2024

*Reviewed By:* RKM, 9/30/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your*



# State of Washington

*basis for this assessment:*

## *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

## *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

## *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

## *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

## *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

**Assess control risk by system and assertion.** This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

## State of Washington

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Financial Statement Audits](#) Planning Guide

Record of Work Done:

#### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation - **MOD**

Occurrence - **MOD**

#### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

##### **Pay1 (Valuation and Occurrence)**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

#### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation - MOD

Occurrence - MOD

#### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

##### **Valuation**

We will use the sampling spreadsheet to determine the amount of transactions for testing. We will use the sample provided by Team IT Audit and re-calculate the total premium associated with our sample using the PEBB/SEBB employer premium, employee premium, tobacco surcharge,

## State of Washington

spouse surcharge, and plan election. The PEBB/SEBB employer/employee premiums, tobacco surcharge and spouse surcharge can be found on the Health Care Authority (HCA) [website](#). The plan election will be provided in the data from Team IT Audit. We will tie the re-calculation of the subscriber's premium (employee and employer portions) to the invoice charged to the participating employer.

### **Occurrence**

We will use the sampling spreadsheet to determine the amount of transactions for testing. We will use the sample provided by Team IT Audit and will test our sample to ensure that the recorded revenue and coverage period occurred in the proper period, by reviewing the invoice.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **F.2.PRG - Premiums and Assessments**

*Procedure Step:* Substantive Test  
*Prepared By:* MRF, 10/3/2024  
*Reviewed By:* RKM, 10/28/2024

Purpose/Conclusion:

#### **Purpose (Occurance):**

To determine whether reported revenues represent actual amounts relating to the period.

#### **Conclusion:**

We determined the recorded revenues represented actual amounts relating to the period.

#### **Purpose (Valuation):**

To determine whether revenues were reported at properly valued or calculated amounts.

#### **Conclusion:**

We determined the revenue was reported at correctly calculated amounts in the Pay1 system.

Testing Strategy:

### **Occurance**

# State of Washington

The following is a list of **considerations** for testing the **occurrence assertion for revenues**. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

## **Cut-Off / Revenue Recognition**

Test transactions recorded in the current period to verify the revenue occurred during the period.

*Transactions recorded at the beginning and end of the current period would generally be considered at highest risk of being improperly recorded in the current period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields.*

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

## **Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

## **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

# State of Washington

## Valuation

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## Calculation

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

## Realizable Value

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

## Estimation / Recognition

Review calculation and support for assumptions of any estimated revenues.

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

## Property Tax Revenues - see separate step

Guidance/Criteria.:

**Add the Guidance/Criteria for each relevant assertion from the TeamStore. You may also include other resources that you used for testing.**

Record of Work Done.:

We worked with IT Audit to obtain monthly subscriber data for PEBB and SEBB from Pay1 [\[Pay1 Revenue Selection - Team IT\]](#) and had them pull our testing sample. The request is documented in HelpDesk #68098.

To gain a better understanding of revenue, we prepared a summary of health insurance revenues. See [\[Health Insurance Activities Updated 2024\]](#).

# State of Washington

## **Substantive tests performed to meet the Existence / Occurrence assertion:**

### **Testing Procedures:**

We reviewed the testing strategy for occurrence. We used the Financial Audit Substantive Statistical Sample spreadsheet with a tolerable misstatement of 7.5%, and a mod assurance level, and determined a planned sample size of 30. This sample is determined with both PEBB and SEBB populations blended together as the process is the same, only the employers are different. We determined we would test 29 additional sample items to obtain an additional level of assurance for both populations, 29 in PEBB and 30 in SEBB. Team IT Audit requested the total data population from HCA's database, and randomly selected the transactions for testing.

We provided our revenue sample to Rita Homan, Deputy Accounting Section Manager. She provided us the Pay1 invoices detailing the coverage period and the billing date. We reviewed the dates for the selected charges to determine if the coverage period and billing was within the proper period.

We tested the sample for the following attributes:

Did the recorded revenue earned within fiscal year ended June 30, 2024?

Was the coverage period within fiscal year ended June 30, 2024?

**Testing Results:** [CONFIDENTIAL DATA\_FS Sampling]. We tested our sample to determine if they represented actual amounts relating to the period and noted **no** exceptions.

## **Substantive tests performed to meet the Valuation assertion:**

### **Testing Procedures:**

We used the same sample of 59 transactions to test for the valuation assertion by recalculating the total premium for each subscriber based on their elections and comparing it to the invoiced amount in the Pay1 system. The PEBB/SEBB employer/employee premiums, tobacco surcharge and spouse surcharge were found on the Health Care Authority (HCA) [website](#). The plan election data was provided in the data from Team IT Audit. The Pay1 invoice documentation was provided by Rita Homan, Deputy Accounting Section Manager. We tied the re-calculation of the subscriber's premium (employee and employer portions) to the invoice charged to the participating employer.

We tested our sample for the following attribute:

Did Pay1 accurately calculate the subscriber's premium?

**Testing Results:** [CONFIDENTIAL DATA\_FS Sampling]. We tested our sample to determine if they were reported at properly valued or calculated amounts and noted **no** exceptions.

## **F.2.PRG - Premiums and Assessments**

# State of Washington

*Procedure Step:* Pay1 Revenue Selection - Team IT  
*Prepared By:* PS, 8/14/2024  
*Reviewed By:* RKM, 10/28/2024

## Purpose/Conclusion:

### **Purpose:**

For Team IT Audit to select random samples related to state employee health care information as requested by Team Financial Audit.

### **Conclusion:**

Team IT Audit has selected and provided random samples related to state employee health care information as requested by Team Financial Audit.

## Testing Strategy:

## Guidance/Criteria:

## Record of Work Done:

### **Data Analysis Request**

Michi Fields from Team Financial Audit has submitted helpdesk 68098 to request for the following items:

1. Help obtaining monthly Pay1 data (census data and billing data for PEBB and SEBB)
2. Provide Pay1 data in a format so we can make selections or have Team IT make selections for recalculating billings (amounts calculated by Pay1)

The audit team also provided the following information:

1. WHO: All active PEBB and SEBB subscribers (all participating employers - state, local governments, school districts, local governments, etc.). Please include the participating employer types. We do NOT want retirees. **Note:** We want subscribers for all months. It might be helpful to clarify if the subscriber will appear for each month they are in PEBB and SEBB and their respective elections. Elections can change



# State of Washington

throughout the year. Election may not be consistent through the whole year.

2. YEAR: Fiscal year ended June 30, 2024 (07/01/2023 - 06/30/2024). **Note:** We would like to receive the data once all is available- probably late July.

3. WHAT FIELDS: Basic subscriber information to ensure traceability. Likely need SSN, name, employer/agency, tier (subscriber only, spouse, full family, etc.), election types for all insurances and benefits.

4. OTHER: additional fees or surcharges (tobacco surcharge and spouse surcharge).

5. PHI/PPI TO EXCLUDE: We do not expect to need dependent SSNs or DOBs. We want to be able to filter non-material participating employer types to simplify testing.

We do NOT need additional selections for control confirmations this year.

## Test Objective

The audit team wants to confirm health insurance billings made during fiscal year 2024 were made at the appropriate amounts. They would like to select transactions from Pay1 data to recalculate billings (amounts calculated by Pay1).

## Methodology

Based upon this request, we will complete the following steps:

Request and obtain from HCA the Pay1 FY2024 data; census and billing data for PEBB and SEBB.

Import the datasets into SQL and perform data reliability checks to confirm that the data received are complete and accurate.

Work with Team FA to determine the criteria for the sampling population, as well as the number of samples.

Pull samples from the data and provide to Team FA.

As we proceed with our testing, we will adjust these steps as needed.

## Data Requests

In order to complete the requested testing, two datasets are required, both from HCA's Pay1 system. One will consist of billings related with state employee health benefits and the other will be the enrollment/census information related to state employee health benefits. This request was attached to the ACFR work order for FY 2024.

HCA provided billings files on August 6th, 2024, and enrollments files on August 5th, 2024. The requested files were provided by Will Sogge,

# State of Washington

External Audit Liaison. We received the following:

- 12 PEBB billing files (one for each month of the fiscal year)
- 12 SEBB billing files (one for each month of the fiscal year)
- PEBB enrollment file
- SEBB enrollment file

Enrollment reference file. This included data definitions, record counts, and field names included in the enrollment files.

Additionally, we also have billing/eligibility field descriptions received from prior year audits, which can be seen at [Pay1 Premiums Billed Data Layout](#) and [PEBB Eligibility Monthly File Field Descriptions](#) (Purpose/conclusion: To document the PEBB Eligibility field descriptions Source: Allen Hall, HCA IT Data Management). Also obtained a list of carrier codes not defined in data layout documents, see [AdditionalCarrierCodes](#).

## **Data Reliability**

We have performed procedures to verify that the data received is complete and accurate. These procedures written in SQL are at [FY24 PEBB SEBB Enrollment DataReliability](#) (PEBB and SEBB enrollment reliability) and [FY24 PEBB SEBB Billings DataReliability](#) (PEBB and SEBB billings reliability). HCA has also gave us a reference table for key data fields at [Reference Tables - FY24](#) Below is a summary of the checks completed:

Verify fields have expected/reasonable values based upon our request and the file layouts.

Verify counts of certain fields remain consistent throughout the year.

Comparisons between the billings and enrollment datasets to identify any differences in the employees included.

The following describes items of note identified during our reliability checks:

There are billing transactions with coverage period outside of the fiscal year. They may be included to show that there are credits associated with these billings.

All employees in PEBB enrollment file are in the billing file but 1 employee in the SEBB enrollment file is not the billing file. From prior year discussions with HCA, this may be due to SSN changes since the enrollment file is a picture in time, whereas the billings are dynamic.

3294 PEBB employees and 2416 SEBB employees are in the billings files but not in the enrollment files. Some of the billings are for coverage periods outside of FY24 and there are many credits for current and prior periods that created a net \$0 billing amount. From prior year discussions with HCA, this is likely due to the enrollment file being a picture in time. In browsing the billing files, we see transactions dates for credits between the enrollment update dates (around the 23rd of the month). It is likely the individuals were

## State of Washington

enrolled at the time of the billing, but not at the time the enrollment table was updated. If one of these employees is selected for testing, we may need to obtain enrollment information from HCA for that particular employee.

Within the billing data, some employees appear in both the PEBB and SEBB populations. As seen in other cases, many of these situations appear to include corrections. However, some employees can also be dual eligible and each entity will pay a portion of the benefits. What we are seeing aligns with these expectations.

Based upon our procedures, we have determined the data appears to be complete and accurate for our testing purposes. We will continue to look for signs of incomplete or inaccurate information as we perform our testing.

### **Data Analysis Testing**

The audit team requested 29 PEBB samples and 30 SEBB samples. We will create two populations as follows:

1. PEBB billing population will consist of:  
Distinct subscriber SSN and coverage month.  
Eligibility Type Y (active state and higher-education employees)  
Include all transaction codes (including credits).
2. SEBB billing population will consist of:  
Distinct subscriber SSN and coverage month.  
Eligibility Type Z (active SEBB).  
Include all transaction codes (including credits).

IT Audit created SQL queries to build the population and pull the samples. For each selected employee, we also pulled all associated billing records. Our queries can be seen at [SampleSelection\\_Queries](#).

Throughout the above queries, we performed checks to verify the completeness of our results. Based upon our checks, we consider the results to be complete and accurate based upon the request.

### **Data Analysis Results**

The results of our testing were provided to Team FA in an Excel spreadsheets titled "!2024\_PEBB\_SEBB\_Sample\_Selections" via our internal network. These results contain CONFIDENTIAL INFORMATION. The spreadsheets are password protected and the password is based on the pattern in the DA password safe. The following result tables were included in the spreadsheets:

[Billing Recalculation Samples](#)

## State of Washington

1. PEBB samples with summary billing and enrollment information (73 records)
2. SEBB samples with summary billing and enrollment information (32 records)
3. PEBB detail billing records associated with selected employees (162 records)
4. SEBB detail billing records associated with selected employees (155 records)

We also provided the audit team with the total record counts associated with the PEBB and SEBB populations created for pulling samples. The total record counts were 1,809,168 for PEBB and 1,840,368 for SEBB and included in the sample selection Excel file.

### F.3.PRG - Premiums and Claims

*Procedure Step:* Summary & Conclusion

*Prepared By:* EZM, 10/1/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

#### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

#### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

## State of Washington

*If the results of substantive testing indicate a need to change control risk, auditors should also update the [Permanent File](#) by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

## State of Washington

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

No, the results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

Yes, the quality and quantity of evidence obtained was sufficient and appropriate.

### **F.3.PR.G - Premiums and Claims**

*Procedure Step:* Understanding of Line Item

*Prepared By:* EZM, 5/22/2024

*Reviewed By:* RKM, 6/5/2024

# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new

## State of Washington

one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

We noted **no** prior audit exceptions.

#### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)]. Our understanding applies to the health insurance opinion unit premiums and claims expense (sub-object NH Health Services Benefits) and the government wide statements for health insurance expenses. We noted the most significant sub-object for the government-wide expense was sub-object NH. We analyzed the expenditure amounts in the line item lead sheet and identified funds 493 (School Employees' Insurance Account) and 721 (Public Employees' and Retirees Insurance Account) as the significant funds for this line item. We also noted that the fund percentage compositions were in line with FY22. There were dollar amount increases for fund 493, and decreases for fund 721, between the two years, but not excessive when considering the nature of health insurance costs.

See understanding of Employee and Retiree Benefits (ERB) operations at []. ERB managed PEBB and SEBB. ERB offers comprehensive medical (pharmacy and medical), vision, dental, life (basic and supplemental), accidental death and dismemberment (AD&D, basic and supplemental), and



## State of Washington

long-term disability (LTD, basic and supplemental) insurances. ERB also offers dependent care assistance program (DCAP) and medical flexible spending arrangements (FSA) benefits.

Premiums and claims includes payments to insurance carriers, benefit vendors, and self-insurance claims. Expenses were ran through sub-object NH for purchased insurance and self-insurance. Regence is the third-party administrator (TPA) for PEBB and SEBB medical self-insurance benefits offered under Uniform Medical Plan. Regence bills HCA weekly claims for PEBB and SEBB subscribers. MODA is the TPA for pharmaceutical claims and bills HCA about every other week. Delta Dental is the TPA for dental claims. Administrative fees for TPAs (based on contracted amounts and performance requirements) are paid monthly.

Adjustments to incurred but not reported (IBNR) liabilities are offset in premiums and claims (sub-object NH). See [\[Summary & Conclusion\]](#) for IBNR understanding. IBNR calculations are based on actuary studies prepared by Milliman quarterly.

In FY20, HCA (ERB Division) was charged with providing health insurance and other employee benefit type insurance to school districts and other related local governments (i.e. educational service districts) across the state and established SEBB. Benefits started January 2020, which made FY21 the first full year that included SEBB benefits.

We identified no unusual or unexpected elements, amounts, or changes that may indicate risk.

**(3) Updates to Significant Account Matrix:**

None.

### **F.3.PR.G - Premiums and Claims**

*Procedure Step:* Controls - AFRS

*Prepared By:* EZM, 5/3/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion.*
----------------------

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

# State of Washington

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

## The following procedures are required for all material systems:

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

## State of Washington

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- Initiation:* How are transactions initiated?
- Authorization:* How are transactions and accounting record maintenance authorized?
- Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Material Balance(s) and Assertions**

Internal controls in the AFRS address the following balance(s):

Health Insurance - Premiums and Claims

Business-Type Activities - Health Insurance - Expenses

For the following assertions:

Occurrence - There is a risk that expenses for payments of claims were not supported by invoices or weekly claims requests to support real obligations incurred during the period.

Valuation (related to the IBNR adjustments only) - The offset to incurred but not reported (IBNR) adjustments were made in premium and claims expenses. There is a risk the adjustments were not supported by an actuary report prepared by a qualified and competent actuary using appropriate assumptions. There is also a risk the actuary report was not calculated based on accurate information provided by HCA or complete claims data.

## **Gain an Understanding of Internal Controls**

We met with the following HCA staff members on April 26, 2024 to gain an understanding of Premiums and Claims:

Rita Homan, Deputy Accounting Section Manager

Sara Whitley, ERB Finance Manager

Lisa Kolle, PEB Accounting Manager

Grant Stromsdorfer, Pay1 Mainframe Support

# State of Washington

Samantha Zimmerman, Internal Control Officer  
William Sogge, External Audit Liaison

## *Self-Insurance Weekly Claim Payments and Purchased Insurance*

### Self-Insurance

Regence (UMP medical claims third party administrator) bills HCA for claims at least weekly. Regence provides detailed claims data weekly to HCA's IT team via secure file transfer. HCA's IT Team imports the data, normalizes the claims data, and removes the data protected by HIPPA (claim numbers, claim/procedure coding, and other patient data). Subscriber social security numbers are retained with the data to ensure claim transactions are tied to a specific subscriber. HCA IT team then loads the data into a SQL database (Microsoft Access)

The ERB accounting department receives summarized weekly claim invoices from Regence via email. Summarized invoices are remitted to ensure minimal HIPPA protected data is generated. An Employee and Retiree Benefits (ERB) Fiscal Analyst 3 or 4 reviews the invoice and runs a report from the claims SQL database for the specific date range. If the report and invoice amounts do not tie, the Fiscal Analyst will contact the internal HCA account manager of that third party administrator and will work with them to reconcile the difference. When the claims detail and invoice tie, the Fiscal Analyst reaches out to the internal HCA account manager to get their approval to pay, and once they offer their approval, the Fiscal Analyst prepares the A19, and the SQL claims report to support the payment. The Fiscal Analyst enters the transaction into AFRS and uploads data into WebAX (HCA's digital documentation system). Katherine Plaquet, Fiscal Analyst 5, reviews and releases the transactions in AFRS. She reviews the transactions to ensure they occurred, were supported by appropriate documentation, and that coding and amounts were accurate **(Key Control #1 - Occurrence - Manual)**.

### Purchased Insurance

Typically, payments to purchased insurance carriers are automatically calculated and manually processed within Pay1. See the Pay1 control understanding at the "Controls - Pay 1" step. If Pay1 is unable to process the payments to purchased insurance carriers for any reason, such as, credits on accounts from prior period, or Metlife payments rounding to 3 decimal places, a Fiscal Analyst 4 will prepare the payment to purchased insurance carriers by using an A19, H.47/F.47 Pay1 screens, and Carrier Payment spreadsheets to determine the payment amounts. At the end of each month, if there are any manual payments that need to be processed during that month, the Fiscal Analyst enters the transaction into AFRS and uploads the source documents into WebAX. The Fiscal Analyst will attach the carrier payment data to an email to the Contract Manager for each carrier for approval. Once Contract Managers approve the payment, Katherine Plaquet, Fiscal Analyst 5; Rita Homan, Deputy Accounting Section Manager; or the PEB Accounting Manager reviews the transactions to ensure they occurred, are adequately supported, and the amount was accurate. The Fiscal Analyst 5, Deputy Accounting Section Manager, or PEB Accounting Manager then releases the transactions in AFRS **(Key Control #2 - Occurrence - Manual)**.

### Other Adjustments (Valuation)

See [\[Controls - Actuarial Report\]](#) for understanding and controls related to IBNR adjustments. Adjustments to the IBNR liability were offset with adjustments to self-insurance medical claims.

# State of Washington

## How Transactions are Recorded in AFRS:

The Fiscal Analyst enters the transaction into AFRS and uploads data into WebAX. A Fiscal Analyst 5 reviews and releases the transactions in AFRS.

## Key Controls are as Follows:

Key Control #1 - Occurrence (Manual) - For weekly Regence claims invoices (self-insurance), a Fiscal Analyst prepares the A19 and the SQL claims report to support the payment. This is entered into AFRS and uploaded into WebAX. A Fiscal Analyst 5 reviews the transactions to ensure they existed, were supported by appropriate documentation, and that coding and amounts were accurate before releasing into AFRS.

Key Control #2 - Occurrence (Manual) - Monthly, a Fiscal Analyst prepares the payment to purchased insurance carriers by using an A19, H.47/F.47 Pay1 screens, and Carrier Payment spreadsheets to calculate the payment and enters the transaction into AFRS and uploads the data into WebAX. A Fiscal Analyst 5, the Deputy Accounting Section Manager, or the PEB Accounting Manager reviews to ensure the manual batches occurred and the amount is accurate and release the transactions in AFRS.

## Noted Weaknesses are as Follows:

None.

## F.3.PRG - Premiums and Claims

*Procedure Step:* Controls - AFRS

*Prepared By:* EZM, 5/3/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion.\*

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

# State of Washington

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

## State of Washington

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- Initiation:* How are transactions initiated?
- Authorization:* How are transactions and accounting record maintenance authorized?
- Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria.*
---------------------



# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done.
----------------------

## **Material Balance(s) and Assertions**

Internal controls in the AFRS address the following balance(s):

Health Insurance - Premiums and Claims

Business-Type Activities - Health Insurance - Expenses

For the following assertions:

Occurrence - There is a risk that expenses for payments of claims were not supported by invoices or weekly claims requests to support real obligations incurred during the period.

Valuation (related to the IBNR adjustments only) - The offset to incurred but not reported (IBNR) adjustments were made in premium and claims expenses. There is a risk the adjustments were not supported by an actuary report prepared by a qualified and competent actuary using appropriate assumptions. There is also a risk the actuary report was not calculated based on accurate information provided by HCA or complete claims data.

## **Gain an Understanding of Internal Controls**

We met with the following HCA staff members on April 26, 2024 to gain an understanding of Premiums and Claims:

Rita Homan, Deputy Accounting Section Manager

Sara Whitley, ERB Finance Manager

Lisa Kolle, PEB Accounting Manager

Grant Stromsdorfer, Pay1 Mainframe Support

Samantha Zimmerman, Internal Control Officer

William Sogge, External Audit Liaison

## State of Washington

### *Self-Insurance Weekly Claim Payments and Purchased Insurance*

#### Self-Insurance

Regence (UMP medical claims third party administrator) bills HCA for claims at least weekly. Regence provides detailed claims data weekly to HCA's IT team via secure file transfer. HCA's IT Team imports the data, normalizes the claims data, and removes the data protected by HIPPA (claim numbers, claim/procedure coding, and other patient data). Subscriber social security numbers are retained with the data to ensure claim transactions are tied to a specific subscriber. HCA IT team then loads the data into a SQL database (Microsoft Access)

The ERB accounting department receives summarized weekly claim invoices from Regence via email. Summarized invoices are remitted to ensure minimal HIPPA protected data is generated. An Employee and Retiree Benefits (ERB) Fiscal Analyst 3 or 4 reviews the invoice and runs a report from the claims SQL database for the specific date range. If the report and invoice amounts do not tie, the Fiscal Analyst will contact the internal HCA account manager of that third party administrator and will work with them to reconcile the difference. When the claims detail and invoice tie, the Fiscal Analyst reaches out to the internal HCA account manager to get their approval to pay, and once they offer their approval, the Fiscal Analyst prepares the A19, and the SQL claims report to support the payment. The Fiscal Analyst enters the transaction into AFRS and uploads data into WebAX (HCA's digital documentation system). Katherine Plaquet, Fiscal Analyst 5, reviews and releases the transactions in AFRS. She reviews the transactions to ensure they occurred, were supported by appropriate documentation, and that coding and amounts were accurate **(Key Control #1 - Occurrence - Manual)**.

#### Purchased Insurance

Typically, payments to purchased insurance carriers are automatically calculated and manually processed within Pay1. See the Pay1 control understanding at the "Controls - Pay 1" step. If Pay1 is unable to process the payments to purchased insurance carriers for any reason, such as, credits on accounts from prior period, or Metlife payments rounding to 3 decimal places, a Fiscal Analyst 4 will prepare the payment to purchased insurance carriers by using an A19, H.47/F.47 Pay1 screens, and Carrier Payment spreadsheets to determine the payment amounts. At the end of each month, if there are any manual payments that need to be processed during that month, the Fiscal Analyst enters the transaction into AFRS and uploads the source documents into WebAX. The Fiscal Analyst will attach the carrier payment data to an email to the Contract Manager for each carrier for approval. Once Contract Managers approve the payment, Katherine Plaquet, Fiscal Analyst 5; Rita Homan, Deputy Accounting Section Manager; or the PEB Accounting Manager reviews the transactions to ensure they occurred, are adequately supported, and the amount was accurate. The Fiscal Analyst 5, Deputy Accounting Section Manager, or PEB Accounting Manager then releases the transactions in AFRS **(Key Control #2 - Occurrence - Manual)**.

#### Other Adjustments (Valuation)

See [\[Controls - Actuarial Report\]](#) for understanding and controls related to IBNR adjustments. Adjustments to the IBNR liability were offset with adjustments to self-insurance medical claims.

#### **How Transactions are Recorded in AFRS:**

# State of Washington

The Fiscal Analyst enters the transaction into AFRS and uploads data into WebAX. A Fiscal Analyst 5 reviews and releases the transactions in AFRS.

## Key Controls are as Follows:

- Key Control #1 - Occurrence (Manual) - For weekly Regence claims invoices (self-insurance), a Fiscal Analyst prepares the A19 and the SQL claims report to support the payment. This is entered into AFRS and uploaded into WebAX. A Fiscal Analyst 5 reviews the transactions to ensure they existed, were supported by appropriate documentation, and that coding and amounts were accurate before releasing into AFRS.
- Key Control #2 - Occurrence (Manual) - Monthly, a Fiscal Analyst prepares the payment to purchased insurance carriers by using an A19, H.47/F.47 Pay1 screens, and Carrier Payment spreadsheets to calculate the payment and enters the transaction into AFRS and uploads the data into WebAX. A Fiscal Analyst 5, the Deputy Accounting Section Manager, or the PEB Accounting Manager reviews to ensure the manual batches occurred and the amount is accurate and release the transactions in AFRS.

## Noted Weaknesses are as Follows:

None.

## F.3.PRG - Premiums and Claims

*Procedure Step:* Key Control #2 (Manual)  
*Prepared By:* EZM, 5/3/2024  
*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To confirm purchased insurance claims are prepared by a Fiscal Analyst and reviewed by a Fiscal Analyst 5, Deputy Accounting Section Manager, or PEB Accounting Manager (Key Control #2 for AFRS - Occurrence) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

# State of Washington

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control #2 (Occurrence): Monthly, a Fiscal Analyst 3-5 prepares the payment to purchased insurance carriers by using an A19, H.47/F.47 Pay1 screens, and Carrier Payment spreadsheets to calculate the payment, and enters the transaction into AFRS and uploads the data into WebAX. A Fiscal Analyst 5, Deputy Accounting Section Manager, or PEB Accounting Manager reviews to ensure the manual batches occurred and the amount is accurate and release the transactions in AFRS.**

The understanding for this system is documented above in the "Controls - AFRS" step.

### **1. Confirmation of Key Manual Control:**

#### PEBB insurance

We reviewed the A19 for Metlife PEBB purchased insurance claims for the month of December 2023 (document - PA060149) in the amount of \$610,197.18, which was prepared by Michael Williamson, Fiscal Analyst 4, and approved by Margee Thompson, PEB Accounting Manager. The payment to Metlife was the only manually processed payment for PEBB purchased insurance in the month of December 2023. We noted the A19, PEBB Carrier payment spreadsheet, and H.47 screenshot from Pay1 totals tied with no exceptions. We also reviewed email correspondence of approval from Kimberly Gazard, Senior Account Manager. **No issues noted.**

#### SEBB insurance

We reviewed the A19 for Metlife SEBB purchased insurance claims for the month of December 2023 (document - SA060072) in the amount of \$592,182.15, which was prepared by Oanh Pham, FA 3, and approved by Margee Thompson, PEB Accounting Manager. The payment to Metlife was the only manually processed payment for SEBB purchased insurance in the month of December 2023. We noted the A19, Carrier payment spreadsheet, and F.47 screenshot from Pay1 totals tied with no exceptions. We also reviewed email correspondence of approval from the Contract Managers: Kimberly Gazard, Senior Account Manager, Beth Heston, Senior Account Manager, and Christine Davis, Senior Account Manager. **No issues noted.**

### **Noted Weaknesses are as follows:**

None.

# State of Washington

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.3.PRG - Premiums and Claims**

*Procedure Step:* Controls - Pay1

*Prepared By:* EZM, 5/3/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.  
In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.

## State of Washington

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

Who or what initiates the control

When (or how often) is the control applied

Who performs the control

As needed, the experience, knowledge and attitude of the person applying the control

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

How the key control is documented or evidenced



## State of Washington

If not obvious from the description, how the control prevents or timely detects and corrects misstatements  
Any exceptions or alternative processing to the normal process  
What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

# State of Washington

Record of Work Done:

## **Material Balance(s) and Assertions**

Internal controls in the AFRS address the following balance(s):

Health Insurance - Premiums and Claims

Business-Type Activities - Health Insurance - Expenses

For the following assertions:

Occurrence - There is a risk that expenses for payments of claims were not supported by invoices or weekly claims requests to support real obligations incurred during the period.

Valuation (related to the IBNR adjustments only) - The offset to incurred but not reported (IBNR) adjustments were made in premium and claims expenses. There is a risk the adjustments were not supported by an actuary report prepared by a qualified and competent actuary using appropriate assumptions. There is also a risk the actuary report was not calculated based on accurate information provided by HCA or complete claims data.

## **Gain an Understanding of Internal Controls**

We met with the following HCA staff members on April 26, 2024 to gain an understanding of internal controls:

Rita Homan, Deputy Accounting Section Manager

Sara Whitley, ERB Finance Manager

Lisa Kolle, PEB Accounting Manager

Grant Stromsdorfer, Pay1 Mainframe Support

Samantha Zimmerman, Internal Control Officer

William Sogge, External Audit Liaison

## **Reconciliation of Subscribers**

Relation to Balance:

The reconciliation ensured amounts billed by Regence for claims were legitimate expenses for subscribers and that expenses existed. This allowed HCA to rely on summary invoices when paying for weekly claims to Regence.

## **Self-Insurance**

On a quarterly basis, Regence and HCA reconcile subscribers by plan elections (**Key Control #1 - Occurrence - Manual**). Regence starts the process by comparing monthly subscribers from Pay1 to Regence's records. Regence then provides HCA's Outreach and Training IT team (O&T) with exceptions. HCA's O&T team reviews the exceptions and makes corrections as necessary in Pay1. The O&T team may then request the Pay1 team send the corrected information back to Regence. This process is repeated as necessary. Regence corrects their data to ensure it matches

## State of Washington

Pay1 elections, which ensures that medical claims paid by Regence are only for eligible subscribers. Regence sends completed census data to MODA, UMP's pharmaceutical Third Party Administrator (TPA), to ensure pharmaceutical subscribers are correct.

### Purchased Insurance

Payments to purchased insurance vendors are based on Pay1 census data, contracted rates, and any corrections made in the prior month (i.e. special open enrollment events - marriage, birth, death). Typically, payments to purchased insurance carriers are automatically calculated, and manually processed within Pay1 using the H.47 screen from PEBB and the F.47 screen from SEBB.

Monthly in Pay1, when HCA goes to invoice purchased insurance carriers (23rd of each month) a Fiscal Analyst 4 will review the payment summary from the H.47 and F.47 screens and reconcile this amount to a SQL query to ensure the amounts match. If the amounts match, the Fiscal Analyst 4 will upload source documents to WebAX and send an email with the payment information for review to the Contract Managers and the Fiscal Analyst 5, Deputy Accounting Section Manager, or the PEB Accounting Manager, who reviews the source documents to ensure the amount is for the correct month and the amount is accurate and approves the release of the payment (**Key Control #2 - Occurrence - Manual**). The Fiscal Analyst 4 will then release the payment in Pay1. Pay1 will automatically upload the transaction data to AFRS through a nightly upload. For purchased insurance payments that cannot be processed in Pay1 due to credits on the account, or most Metlife Insurance payments, Fiscal Analysts must manually process these payments in AFRS. See the manual process in the "Controls - AFRS" step.

### Other Adjustments (Valuation)

See [Controls - Actuarial Report] for understanding and controls related to IBNR adjustments. Adjustments to the IBNR liability were offset with adjustments to self-insurance medical claims.

### **How Transactions are Recorded in AFRS:**

Invoices for weekly claim payments (self-insurance) are manually entered into AFRS. See the "Controls - AFRS" step.

Monthly premium payments (purchased insurance) processed in Pay1 are automatically uploaded into AFRS through a nightly batch.

No financial transactions directly related to the enrollment or census data reconciliation.

### **Key Controls are as Follows:**

Key Control #1 (Occurrence - Manual) - Quarterly, census data is reconciled between PAY1 and Regence's (UMP TPA) records to ensure claims paid by Regence were for PEBB Uniform Medical Plan (UMP) subscribers.

Key Control #2 (Occurrence - Manual) - Monthly, a Fiscal Analyst 4 or above compares the H.47 and F.47 screens in Pay1 to a SQL query to ensure the automatically batched amounts match and the Contract Managers and Fiscal Analyst 5, Deputy Accounting Section Manager, or PEB Accounting Manager, review to ensure the amount is for the correct month and is accurate before processing the payment.

# State of Washington

## Noted Weaknesses are as Follows:

None.

### F.3.PR.G - Premiums and Claims

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* EZM, 8/30/2024

*Reviewed By:* RKM, 9/9/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm that census data is reconciled quarterly between Pay1 and Regence's records to ensure claims paid by Regence were for PEBB Uniform Medical Plan subscribers (**key control #1 for Pay1**) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

## State of Washington

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the*

## State of Washington

*appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #1 (Occurrence): Quarterly, census data is reconciled between PAY1 and Regence's (UMP TPA) records to ensure claims paid by Regence were for PEBB Uniform Medical Plan (UMP) subscribers.**

The understanding for this system is documented above in the "Controls - Pay1" step.

### **1. Confirmation of Key Manual Control:**

## State of Washington

On May 23, 2024, we met with the following HCA staff members so they could walk us through the quarterly census data reconciliation file (excel file titled "Final – Open Items – 1<sup>st</sup> Quarter 2024 HCA Audit") for January 2024 through March 2024:

Rita Homan, Deputy Accounting Section Manager  
Shawna Lang, Section Manager, PEB Portfolio  
Grant Stromsdorfer, Pay1 Mainframe Support  
Lisa Kolle, ERB Accounting Manager  
Kari Summerour, External Audit Manager

We noted this file had three tabs – Audit Discrepancies, Middle Initial Discrepancies, and Suffix Discrepancies. All tabs had columns for Subscriber ID, Carrier Code, Sub SSN, Sub last name, Sub first name, and Audit Issue/Discrepancy. We noted this file contained 159 total accounts with discrepancies between Regence and HCA data (129 in the "Audit Discrepancies" tab and 30 in the "Middle Initial Discrepancies" tab) and Regence described the discrepancies in the "Audit Issue/Discrepancy" column. We inquired with Grant Stromsdorfer, Pay1 Mainframe Support, on whether all of the discrepancies were corrected and he said that correcting these discrepancies was an ongoing daily process between Regence and HCA that is handled through multiple tickets. We inspected an email that showed that, on May 3, 2023, Regence sent over their list of discrepancies to HCA. Because HCA was able to show us documentation that demonstrated that they're actively working with Regence to reconcile subscriber data and resolve any discrepancies, we consider this control to be adequately in place. When we inquired about whether HCA would have these discrepancies fully reconciled as of fiscal year end, Kari Summerour informed us that the O&T team is working on the list of discrepancies with the goal of getting them completed by 6/30/24. Kari stated that when discrepancies are completed, they are removed from the initial spreadsheet, which is how they track how many discrepancies are still outstanding.

On August 30, 2024, we received a spreadsheet titled "Carryover from Q1 2024" which detailed all of the discrepancies between HCA's data and Regence's data. We noted that there were 42 discrepancies still outstanding as of June 30, 2024, and we received email communications between HCA staff and Regence staff showing that they're actively working together on resolving these discrepancies. **No issues noted.**

### **Noted Weaknesses are as follows:**

None.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

# State of Washington

## F.3.PRG - Premiums and Claims

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* EZM, 5/3/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

**Purpose:**

To confirm HCA's Fiscal Analyst 4s are comparing Pay1 payment screens to SQL queries to ensure amounts match before sending the supporting documents to the Contract Managers and the Accounting Manager or FA5 for review before processing payments for Pay1 (Key Control #2 for Pay1 - Occurrence) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*



## State of Washington

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence*

## State of Washington

*about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #2 (Occurrence): Monthly, a Fiscal Analyst 4 or above compares the H.47 and F.47 screens in Pay1 to a SQL query to ensure the automatically batched amounts match and the Contract Managers and Fiscal Analyst 5, Deputy Accounting Section Manager, or PEB Accounting Manager, review to ensure the amount is for the correct month and is accurate before processing the payment.**

The understanding for this system is documented above in the "Controls - Pay1" step.

**1. Confirmation of Key Manual Control:**  
**PEBB:**

## State of Washington

We received the H.47 screenshot and the PEBB Carrier payment query for the February 2024 purchased insurance payment. We noted the H.47 total carrier amount is \$62,317,873.11, which tied to the SQL query amount without exception. We noted the upload was created by Michael Williamson, Fiscal Analyst 4, and approved by Katherine Plaquet, Fiscal Analyst 5. We also reviewed Contract Manager approvals from Beth Heston, Senior Account Manager, Kimberly Gazard, Senior Account Manager, and Christine Davis, Senior Account Manager, via email. This entire amount was automatically batched. **No issues noted.**

### **SEBB:**

We received the F.47 screenshot and the SEBB Carrier payment query for the February 2024 purchased insurance payment. We noted the F.47 total carrier amount is \$74,349,990.24, which tied to the SQL query amount without exception. We noted the upload was created by Oanh Pham, Fiscal Analyst 4, and approved by Katherine Plaquet, Fiscal Analyst 5. We also reviewed Contract Manager approvals from Beth Heston, Senior Account Manager, Kimberly Gazard, Senior Account Manager, and Christine Davis, Senior Account Manager, via email. This entire amount was automatically batched. **No issues noted.**

### **Noted Weaknesses are as follows:**

None.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **F.3.PRГ - Premiums and Claims**

*Procedure Step:* Risk Assessment

*Prepared By:* EZM, 10/1/2024

*Reviewed By:* CJG, 12/9/2024

Purpose/Conclusion.*
----------------------

# State of Washington

## **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

#### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

#### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

#### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

#### *Inherent Risk due to Misappropriation*

## State of Washington

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

# State of Washington

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

## **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Occurrence – **HIGH**

Valuation - **HIGH**

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

AFRS – Occurrence, Valuation

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

# State of Washington

Pay1 – Occurrence, Valuation

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Occurrence – **HIGH**

Valuation – **HIGH**

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

### **Occurrence**

#### Purchased Insurance

We will test the entire population of 24 purchased insurance payments to vendors. To test each transaction, we will tie out the disbursement in AFRS to HCA's Pay1 system (Pay1 payment summary screens H.47 for PEBB and F.47 for SEBB), to ensure that the payments were valid and recorded in the proper period.

We will also compare the AFRS expenditure amounts for each of the Purchased Insurance monthly payments to the Carrier Payment spreadsheets to determine how HCA arrived at the AFRS amounts. If there are any adjustments made to the amounts in the Carrier Payment spreadsheets, we will request supporting documentation and explanations for adjustments made that are above the floor.

#### Self-Insurance

We will use detailed GL activity (Webi) and filter the data by subsubobject, GL 6505 accrued expenses and GL 6510 cash expenses to determine our population. We will use the sampling spreadsheet to determine our sample size. To test each transaction we will review HCA's summary of vendor invoice by plan and subsubobject, HCA's Voucher Distribution Form (A19) and the vendors invoice (I.e. Regence, Moda, and Delta Dental), subtotaled by plans offered for PEBB/SEBB, to ensure that the transactions are valid and recorded in the proper fiscal year.

We will also compare the AFRS expenditure amounts for each of the invoices we selected for testing to the weekly/monthly claims data reports that HCA used in order to arrive at the expenditure amounts. If there are any adjustments made to the claims data report figures in order to arrive at the expenditure amounts, we will request supporting documentation and explanations for adjustments that are above the floor.

## State of Washington

**Valuation** - See [Risk Assessment] for incurred but not paid (IBNP) testing strategy. Adjustments made to the IBNP liability were offset in claims expenses. No additional work planned for expense of IBNP adjustments. Note, HCA called the incurred but not paid (IBNP) liability the incurred but not recorded (IBNR) liability. IBNP and IBNR were used interchangeably.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### F.3.PRG - Premiums and Claims

*Procedure Step:* Substantive Test

*Prepared By:* EZM, 10/1/2024

*Reviewed By:* CJG, 12/9/2024

Purpose/Conclusion.:

#### **Purpose:**

To determine whether reported expenses/expenditures represent real obligations incurred during the period.  
To determine whether expenses/expenditures were reported at properly valued or calculated amounts.

#### **Conclusion:**

We determined that reported expenses/expenditures represent real obligations incurred during the period.  
We determined that expenses/expenditures were reported at properly valued or calculated amounts.

Testing Strategy.:

#### **Occurrence Testing Strategy**

The following is a list of **considerations** for testing the occurrence assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

#### **Detail Roll-up**

Compare totals from general ledger to accounts payable, payroll or other subsidiary software modules.



## State of Washington

Review the government's reconciliation of general ledger to subsidiary systems.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

### **Fictitious expenses**

Search for manual journal entries that debit (increase) expenditures. Consider testing if any risk indicators are noted.

Evaluate liabilities directly related to expenses for existence. See the existence steps for current and non-current liabilities for testing considerations.

*For example, if the entity reports a self-insurance liability, the auditor might evaluate whether the change in the liability (and associated expense) occurred. Similarly, if a new liability was reported, evaluate whether that liability (and associated expense) actually exists.*

If the entity reconciles recorded revenues and expenses to bank activity, then review monthly reconciliations and evaluate or test reconciling items.

If entity uses a warrant clearing account or payroll clearing account, review the entity's year-end reconciliation of recorded vendor payments and/or payroll payments with disbursements from the clearing account(s).

Test a sample of expenses/expenditures to determine whether the transaction was valid.

Perform analytical procedures on payroll expenses/expenditures. The analysis should include development of an expectation of what payroll should be in the current year due to changes in employees, COLAs, benefits, etc.

Test payroll to see if transactions are properly charged

### **Invalid, Unallowable or Fraudulent Expenses**

*See the testing strategy considerations in the Rights & Obligations step.*

### **Improper Expense Recognition**

Test selected or sampled expenditures recorded in the current period to verify the expense was recorded for the proper period.

*Transactions at the beginning and end of the period would generally be considered at highest risk of being improperly recorded in the current period. Auditors should consider scanning transactions recorded during these timeframes to identify high risk transactions.*

### **Incorrectly recording expenses that do not meet GAAP criteria**

## State of Washington

Review the entity's schedule cross-walking the financial statements to the general ledger and check that any transactions among consolidated funds are eliminated.

Check that transactions among governmental funds and transactions among proprietary funds are eliminated on the government-wide statements.

### **Interfund Expenses**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

### Valuation Testing Strategy

The following is a list of **considerations** for testing the valuation assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests:

- Verify that payroll calculations are correct.

- If not already covered as part of control testing, verify that payroll software used correct rates.

- If not already covered as part of control testing, verify that accounts payable software used correct rates for calculating sales tax.

- Review calculation of any estimated expenses.

- Review related-party transactions to determine whether expense/expenditure transactions were correctly calculated.

### **Landfill Closure & Post-Closure Expenses**

*See the valuation testing strategy for non-current liabilities..*

**OPEB** - Auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - Auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

Guidance/Criteria:
--------------------

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.8.6](#) Use of Payroll and Claims Funds**

# State of Washington

Record of Work Done:

## **Substantive tests performed to meet the Occurrence assertion:**

### Testing Procedures:

We reviewed the testing strategy for occurrence. We tested the self-insurance and purchased insurance transactions for the occurrence assertion as follows:

### Purchased Insurance

For purchased insurance, we determined we would test all of the transactions in the population, as the population was small and the support was readily available. To test each transaction, we tied out the disbursement in AFRS to HCA's Pay1 system (Pay1 payment summary screens H.47 for PEBB and F.47 for SEBB) and reviewed the month of service to ensure that the payments were valid and recorded in the proper period. We tested the entire purchased insurance population for the following attributes:

Did the recorded expense occur within FYE June 30, 2024?

Did the recorded expense in AFRS tie to the Pay1 H.47 (PEBB) or F.47 (SEBB) screenshot?

We also compared the AFRS expenditure amounts for each of the invoices we selected for testing to the weekly/monthly claims data reports that HCA used in order to arrive at the expenditure amounts, and the figures tied without exception. We noted that there were some large adjustments (over \$110k, which is our floor) made to the invoice amounts - we requested support for these adjustments in order to confirm that the amounts were supported by adequate documentation. We reviewed the documentation we received, which were supplemental invoices from the third party administrators, and the amounts in the invoices tied to the adjustment amounts in the weekly/monthly claims data reports without exception.

We also compared the AFRS expenditure amounts for each of the Purchased Insurance monthly payments to the Carrier Payment spreadsheets to determine how HCA arrived at the AFRS amounts. We noted that there were two adjustments made to October and November 2023 monthly payments, totaling \$13.365 million and \$13.189 million, respectively. We requested support for these amounts and received a "SEBB 2022 Risk Adjustment" spreadsheet that supported these amounts. We noted that the amount was made up of 2022 SEBB risk adjustment transfers for Kaiser Foundation Health Plan of WA (KPWA), Kaiser Foundation Health Plan of WA Options (KPWAO), Kaiser Foundation Health Plan of the Northwest (KPNW), and Premera.

### Self-Insurance

For self-insurance, we used the sampling spreadsheet (7.5% tolerable misstatement, assurance set to high) to determine our sample size. While we had an initial sample size of 38, we decided to test a sample that aligned with a very high level of assurance, due to the fact that the Premiums & Claims balance significantly increased from the prior year (in FY23, it was \$3.8 billion, and in FY24, it's \$5 billion). To test each transaction we reviewed HCA's summary of vendor invoices by plan and subsubobject, HCA's Voucher Distribution Form (A19) and the vendor's invoice (I.e. Regence, Premera, Moda, and Delta Dental) to determine the month of service, and tied the invoice to the A-19, to ensure that the

## State of Washington

transactions are valid and recorded in the proper fiscal year. We tested each transaction for the following attributes:

(Occurrence) - Did the recorded expense occur within FYE June 30, 2024?

(Occurrence) - Did the recorded expense tie to the documentation from the vendor?

We also compared the AFRS expenditure amounts for each of the invoices we selected for testing to the weekly/monthly claims data reports that HCA used in order to arrive at the expenditure amounts, and the figures tied without exception. We noted that there were some large adjustments (over \$110k, which is our floor) made to the invoice amounts - we requested support for these adjustments in order to confirm that the amounts were supported by adequate documentation. We reviewed the documentation we received, which were supplemental invoices from the third party administrators, and the amounts in the invoices tied to the adjustment amounts in the weekly/monthly claims data reports without exception.

### Testing Results:

Purchased Insurance testing: [\[FS Sampling - Premiums and Claims\]](#).

We tested all of the transactions for the occurrence assertion and we did not note any exceptions.

Self-Insurance testing: [\[FS Sampling - Premiums and Claims\]](#).

We tested this sample for the occurrence assertion and we did not note any exceptions.

### **Substantive tests performed to meet the Valuation assertion:**

#### Testing Procedures:

The valuation risk is related to incurred but not paid (IBNP) adjustments. Our understanding of this area is found in the Claims and Judgments Payable line item found here [\[Understanding of Line Item\]](#). The liability is adjusting subobject NH, health insurance premium and claims expenses. See IBNR testing at [\[Substantive Test\]](#).

### **F.4.PRG - Due From Other Governments**

*Procedure Step:* Summary & Conclusion

*Prepared By:* MRF, 10/1/2024

*Reviewed By:* RKM, 11/24/2024

Purpose/Conclusion:
---------------------

# State of Washington

## **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

## **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### **Information to be used as audit evidence:**

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

## State of Washington

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

Is information precise enough to catch if misstatements exceeded the tolerable level?

Is information detailed enough to conclude on whether or not there were misstatements?

Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?

How did misstatements occur and how often might they occur again in the population?

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

# State of Washington

## Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

Risk of Material Misstatement was originally determined to be MAX. We determined we did not need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

## **F.4.PRG - Due From Other Governments**

*Procedure Step:* Understanding of Line Item

*Prepared By:* MRF, 5/22/2024

*Reviewed By:* RKM, 8/20/2024

## Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

We will repeat a recommendation for HCA to improve resources (PAY1 reports, databases, etc.) to facilitate the tracking of invoices, payments, any related adjustments, and batched revenue transactions between PAY1 and AFRS [E: HCA Receivables Lack of Complete Reconciliation Pay1 to AFRS].

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

# State of Washington

## **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

## **STEP 3: Update Material Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding*



# State of Washington

*documented.*

*Talk with the AIC if you identify any changes to the Material Account Matrix.*

Guidance/Criteria:

Record of Work Done:

## **(1) Prior Audit Exceptions:**

During the FY23 audit we found that Pay1 receivable reports (B5519 and B5381) for PEBB and SEBB were not tied out to AFRS by ERB accountants at year end to ensure AFRS amounts were accurate and existed. HCA relied on automatic coding and posting performed by Pay1. HCA ERB relied on cash reconciliations to ensure all cash was accurately recorded in Pay1 and AFRS.

We followed up with Rita Homan, Deputy Accounting Section Manager, on 05/02/2024 regarding this issue. She explained HCA is still in process of implementing resource/report improvements. This includes improving the resources to facilitate the tracking of invoices, payments, any related adjustments, and batched revenue transactions between PAY1 and AFRS. HCA Accounting submitted a request to HCA's IT department for PAY1 receivables data to be loaded to a SQL database to facilitate a full reconciliation between PAY1 receivables and AFRS. It has not yet been completed. We will include this in a recommendation to HCA for FY24. See issue at [\[E: HCA Receivables Lack of Complete Reconciliation Pay1 to AFRS\]](#).

## **(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

Due from Other Governments was reported in the following funds:

Fund 721 - Public Employees' and Retirees Insurance Account - represents about 10% of the total due.

In FY21, MODA pharmaceutical rebates were also included in the Due from Other Governments balance, and made Fund 721 about 30% of the total.

Milliman actuarial services later determined these rebates should be recorded in the "Invoiced But Not Received (IBNR)" balance, which reduced the amount recorded in Fund 721 to about 10% of the total.

HCA expects this policy to continue in FY24 and we do not expect to test fund 721 in Due From Other Governments

Fund 493 - School Employees' Insurance Account - Represents about 90% of the total due from other governments balance.

Based on general HCA Employee and Retiree Benefits (ERB) division understanding, GL 1352 Due from Other Governments included activity from higher education state agencies, and external local governments or political subdivisions (cities, towns, counties, school districts, etc.). HCA managed PEBB and SEBB under the Employee and Retiree Benefits division. See [\[Health Insurance Activities Updated 2024\]](#) for general understanding of ERB operations.

## State of Washington

The Health Insurance opinion unit was new for fiscal year ended 06/30/2021. In prior years, OFM made adjustments to remove retiree activity from PEBB balances to fiduciary funds. Due to GASB 84, retirees were no longer presented in fiduciary activities and reported in a custodial fund (FKE).

### **(3) Updates to Significant Account Matrix:**

We determined no updates to the Significant Account Matrix were necessary.

### **F.4.PR.G - Due From Other Governments**

*Procedure Step:* Controls - Pay1  
*Prepared By:* MRF, 5/6/2024  
*Reviewed By:* RKM, 9/30/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done. We noted the following weakness:

Pay1 receivable reports (B5519 and B5381) for PEBB and SEBB were not tied out to AFRS by ERB accountants at year end to ensure AFRS amounts were accurate and existed. HCA relied on automatic coding and posting performed by Pay1. HCA ERB relied on cash reconciliations to ensure all cash was accurately recorded in Pay1 and AFRS. See issue at [[E: HCA Receivables Lack of Complete Reconciliation Pay1 to AFRS](#)].

# State of Washington

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

## State of Washington

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria.*
---------------------

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done.
----------------------

## **Material Balance(s) and Assertions**

Internal controls in Pay1 address the following balance(s):

Due From Other Governments

For the following assertions:

Existence - There is a risk that recorded receivables are more than source billings or records.

Valuation - There is a risk the receivables have not been properly calculated.

Classification - There is a risk amounts due from state entities have been reported as due from other governments.

## **Gain an Understanding of Internal Controls**

We met with HCA on 5/01/2024 to review controls over accounts receivable and the related allowance for doubtful accounts. We met with the following HCA staff:

Rita Homan, HCA Deputy Accounting Section Manager

Kari Summerour- External Audit Liaison

William Sogge- External Audit Liaison

See [[Health Insurance Activities Updated 2024](#)] for understanding of ERB operations and billing cycles. See [[Premiums and Assessments](#)] for revenue understanding.

## **Background Information**

Public Employee Benefits Board (PEBB) operations are governed by [RCW 41.05](#), [WAC 182-08](#), [WAC 182-12](#), and [WAC 182-16](#). [WAC 182-08-180](#) defined payments are due the first day of the month in which coverage was effective. PEBB subscriber payments are due with 45 days for the first month of COBRA coverage. Continuing payments are considered past due after 30 days. Participating employers and subscribers are given a 30

## State of Washington

day grace period for late payments. Subscribers are retroactively terminated after 60 days of non-payment. Before termination, the Assistant Accounting Section Manager noted HCA made efforts to describe the consequences of retroactive termination and allowed subscribers to establish a payment plan.

School Employee Benefits Board (SEBB) was voted to be PEBB-like by the board and governed under RCW 41.05, WAC 182-30, WAC 182-31, and WAC 182-32. WAC 182-30-040 defined specific payment rules. SEBB premiums are also due the first day of the month in which coverage was effective. SEBB subscriber payments are due with 45 days for the first month of COBRA coverage. Continuing payments are similar to PEBB rules in which payments were due within 30 days and retroactively terminated after 60 days of non-payment. SEBB subscribers are also eligible to establish payments plans if needed to prevent terminations of coverage.

### **Due From Other Governments - GL 1352**

#### **Pay1 Automatic Invoicing**

Pay1 maintains key information for all subscribers and dependents. Participating employers are responsible for accuracy of demographic information and elections maintained in Pay1. Based on elections entered or imported into Pay1 by the participating employer, Pay1 automatically calculates the amount due for each individual subscriber in an itemized monthly bill by SSN. To perform the calculation, Pay1 uses the rate tables that are updated every six months to calculate subscriber premiums. The subscriber premiums are added to the employer premiums to calculate the total amount owed to HCA by subscriber. The employer premiums are determined by the State Index Rate or for Political Sub-Divisions, a contracted rate. The State Index Rate is determined semi-annually by Legislature.

Pay1 then automatically posts calculated revenues and related accounts receivable for PEBB and SEBB based on current month subscriber elections (**Key Control #1 - Automated Interface - Existence/Valuation**). Nightly, PAY1 interfaces with AFRS to post transactions. Calculated invoice amounts are summarized in the HRISD-B5099-R01 report "Invoice Report by Agency". Each day's transactions posted to AFRS from the invoice reports are summarized in the HRISD-B5081-R01 report "Insurance to AFRS Transaction Generation Report". Amounts reported in AFRS tie back to both automated Pay1 reports.

After invoices were created, Pay1 suspended posting the revenues and related receivables until the first of the month for services. In the prior years, receivable reports included the suspended billings under the 0-30 days aging column on receivable reports. Therefore, the June report would include July which would be the suspended billings. For FY22 the report was modified to not include the suspended billings so they would not have to be backed out each month.

Transactions are easily identifiable by transaction codes. We received a OneNote document compiled by Rita Homan that showed the cycles for posting invoiced amounts, receipts, and refunds. Invoices are grouped based on the type of receivable. For example, self pay retiree invoices are posted using TC 12. For transactions posted in relation to the Due From Other Governments Balance (GL 1352), the following transaction codes were used:

52 - To post receivables from governments. Debits 1352 (Due From Other Governments), Credits 3205 (Accrued Revenue)

## State of Washington

92 - To post cash receipts from governments. Debits 7110 (Receipts In-Process), Credits 1352 (Due From Other Governments)

### Cash Receipts

HCA accepted payments from participating employers and subscribers via lock box for self-pay (retirees), COBRA subscribers, and school districts. State agencies and retirees who elected to have their PEBB premiums withheld from their DRS monthly distribution paid via direct transfer automatically executed with transfers from the treasury office.

HCA's lock box and bank accounts were held with US Bank (DES state contract). Every work day, cash lock box reports for PEBB and SEBB were remitted to HCA via secure file transfer. Reports indicated the employer number (agency number) or subscriber number (social security number). HCA imported the banking activity into Pay1 through an automated nightly batch process. Pay1 automatically coded payments to participating employer or subscriber accounts with full AFRS revenue source coding. Cash activity was also automatically sent to AFRS and reduces receivable balances. When Pay1 could not identify the account due to an issue with social security numbers or agency number, the payment was coded to the suspense account. When Pay1 could not identify the account due to a mismatched account type, the payment was coded to 107BSU. Mismatched payments typically occurred when subscribers changed type of accounts. For example, new retirees often remitted their first payment before their retiree account was complete in Pay1 (self-pay) or if a subscriber separated from their respective participating employer and started COBRA coverage.

Employee Retiree Benefits (ERB) division accountants review lockbox reports daily and match payments for completeness and accuracy. The ERB accountants monitor revenues and cash receipts to ensure bills prepared by Pay1 are accurate and match the amounts in AFRS. If the amount in AFRS does not match the amount collected in Pay1, an In-Process Report is automatically generated. This report provides details on any discrepancies between the amount in AFRS to the amount in Pay1. The ERB Accountants review this report daily and address any discrepancies **(Key Control #2 - Manual - Existence/Classification)**. The "Unbalanced In-process Reconciliation Report" report number DLY007 is ran by fiscal staff for transactions in process through the day before. The unbalanced report is reviewed to ensure amounts are posted to the correct fund in the correct amount. If any significant changes are identified, ERB staff track and research incorrectly posted amounts. The automatic bank lockbox reports and posting of revenue in PAY1 are reviewed and confirmed daily at a high level (in-process report has to match what was received by the lockbox that day vs. AFRS entries for each daily lockbox). Lockboxes for PEBB and SEBB employers are additionally reviewed monthly to ensure the correct employer was credited.

### Adjusting Entries - Prepayments/Credit Balances

At the end of the month, Pay1 automatically generated aging reports based on customer type. Pay1 generated the following reports:

- bh#grp.txt
- bh#ind.txt
- pebb#grp.txt
- pebb#ind.txt, PAY1 report HRISD-B5519-R01
- sebb#ind.txt, Pay1 report SEBB-B5519-R01

## State of Washington

excrpt.txt

Reports were reviewed for reasonableness by ERB Fiscal Analyst 4s and reformatted so ERB Fiscal Analyst 2s could manage individual accounts listed. Reports were also converted to Excel for retention purposes. ERB Fiscal Analysts 2 contacted every customer that had a balance greater than 30 days past due and advised them if no payment occurred, they would be terminated from PEBB or SEBB.

The Pay1 receivable reports (B5519 and B5381) for PEBB and SEBB were not tied out to AFRS by ERB accountants at year end to ensure AFRS amounts were accurate and existed. HCA relied on automatic coding and posting performed by Pay1. HCA ERB relied on cash reconciliations to ensure all cash was accurately recorded in Pay1 and AFRS. See issue at [\[E: HCA Receivables Lack of Complete Reconciliation Pay1 to AFRS\]](#).

Monthly, IT generated a printed receivable report from Pay1, HRISD-B5519-R01 and SEBB-B5519-R01. This report summarized all receivables for each customer. Rita Homan, Assistant Accounting Section Manager, reviewed the report manually at the end of every month to ensure the following:

- Significant past due amounts were being followed up on ERB Fiscal Analyst 2s and documented
- Review for errors and other automatic transactions that Pay1 may have posted to customer accounts

FA4s used the 'pebb#ind.txt' file to prepare backup for the unearned journal voucher (reversing JV). Receivable data (payments) was filtered to identify subscriber accounts with credits by revenue source code. The FA4 used the Excel workbook to prepare the journal voucher. The FA5s, ERB Accounting Manager, and Assistant Accounting Section Manager were allowed reviewers to post the adjustment. JVs were reviewed to ensure the revenue source codes used were complete and receivable balances were accurate and represented actual amounts from Pay1 **(Key Control #3 – Manual – Valuation/Classification)**.

The same PEBB procedures noted above were used for SEBB reports and the SEBB unearned revenue adjustment (reversing JV). SEBB had the same review controls as PEBB.

### **Adjusting Entries - Write-Offs and Allowance for Doubtful Accounts**

Receivable balances over 90 days were considered uncollectible and reported in allowance for doubtful accounts. Write-offs were also based off of the monthly report "Monthly Group Aging Report Summary" (Pay1 report HRISD-B5519-R01). The ERB Fiscal Analyst (FA) 4 converted the text file into Excel. The FA4 totaled the receivables over 90 days past due for self-pay customers and retirees. The FA4 compared the month end and beginning of the month balances to determine the appropriate adjustment needed. The FA4 prepared the monthly journal voucher. The FA5, Assistant Accounting Section Manager, or ERB Accounting Section Manager reviewed the journal vouchers and related workpapers to ensure the accuracy of the adjustment **(Key Control #4 - Manual - Valuation/Classification)**.

Rita explained write-offs can also be made if they are for tolerated amounts. Tolerated amounts are based on the type of payor and history with payments. Write-offs are made in the H.11 screen within Pay1, where all adjustments are made. Activity is documented within H.11 including who



## State of Washington

made the adjustment and comments to justify the write-off. At month end, Pay1 also generates a report HRISD-B5217-R01 and SEBB-B5217-R01 "Write-Off Report" that summarizes those write-offs to be included in the monthly adjusting JV. PEBB and SEBB did not sell off uncollectible receivables. When subscribers were terminated for non-payment, Pay1 recorded a write-off for the receivable and automatically posted the transaction in AFRS.

If participating employers or subscribers did not pay the full premium (including surcharges due), ERB fiscal analysts were allowed to write-off insignificant amounts (insignificant shortfalls). Insignificant amounts were defined in WAC 182-05-015 and considered amounts less than \$50 or 10% of the premium. Write-offs with comments were summarized and reviewed in the monthly adjusting journal entry for the allowance for doubtful accounts.

### **Classification of Receivables**

The Deputy Accounting Section Manager noted classification of receivables was based on the customer type and how customers paid. She also noted PEBB, the plan other state agencies were members of, did not use interagency due to and due from accounts. All participating employers in the PEBB and SEBB plans were governments. Retiree accounts, amounts were reported as Due from Other Governments because a significant amount of retirees had their premiums withheld from their respective monthly DRS pension distribution. As of June 30, 2021, retirees were not included in the health insurance opinion unit. Retiree activity was reported in a custodial fund (FKE).

### **How transactions are recorded in AFRS:**

Pay1 automatically posted invoices and applied cash receipts to customers' receivable accounts.

For monthly adjustments, ERB accountants use journal vouchers based on Pay1 reports to reclassify and adjust receivable balances.

### **Key controls are as follows:**

**Key Control #1 (Automated Interface - Existence/Valuation):** Pay1 automatically posts calculated revenues and related accounts receivable for PEBB and SEBB based on current month subscriber elections.

**Key Control #2 (Manual - Existence/Classification):** Daily, ERB accountants review payments automatically processed and not automatically processed, in Pay1, and reconcile payments to AFRS to ensure that revenues/receivables exist and are accurately classified for the Pay1 System.

**Key Control #3 (Manual - Valuation/Classification):** Monthly, ERB FA4s manually adjusted receivables related to PEBB/SEBB premiums by journal voucher. Adjusting entries were used to record prepayments and credit balances for groups based on Pay1 report HRISD-B5519-R01 and SEBB-B5519-R01. The entry is reviewed by the FA5, ERB Accounting Section Manager, or Deputy Accounting Section Manager to ensure accuracy and classification of adjustments.

**Key Control #4 (Manual - Valuation/Classification):** Monthly, ERB FA4s manually adjusted receivables related to PEBB/SEBB premiums by journal voucher. Adjusting entries were used to record allowance for doubtful accounts and write-offs based on Pay1 report HRISD-B5519-R01 and SEBB-B5519-R01. The entry is reviewed by the FA5, ERB Accounting Section Manager, or Deputy Accounting Section Manager to ensure accuracy and classification of adjustments.

# State of Washington

## Noted Weaknesses are as Follows:

PAY1/AFRS Reconciliation - Pay1 receivable reports (B5519 and B5381) for PEBB and SEBB were not tied out to AFRS by ERB accountants at year end to ensure AFRS amounts were accurate and existed. HCA relied on automatic coding and posting performed by Pay1. HCA ERB relied on cash reconciliations to ensure all cash was accurately recorded in Pay1 and AFRS. See issue at [\[E: HCA Receivables Lack of Complete Reconciliation Pay1 to AFRS\]](#).

## F.4.PRG - Due From Other Governments

*Procedure Step:* Key Control #1 (Automated)

*Prepared By:* MRF, 5/24/2024

*Reviewed By:* RKM, 6/5/2024

### Purpose/Conclusion:

#### **Purpose:**

To determine whether Pay1 automatically calculates and prepares monthly billings based on current month subscriber elections maintained in Pay1, and prepares billings based on approved employer and employee rates (**key control #1 for Pay1**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - Pay1\]](#).

### Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

# State of Washington

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

## Software Calculation:

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

## Software Calculation:

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

## State of Washington

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

## State of Washington

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

# State of Washington

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **Due From Other Governments - Automated Interface - Existence/Valuation**

**Key Control 1 - (Existence/Valuation): Pay1 automatically posts calculated revenues and related accounts receivable for PEBB and SEBB based on current month subscriber elections.**

## **STEP 1: Understand Automated Key Control**

The understanding for this key control is documented above in the "Controls - Pay1" step.

## **STEP 2: Confirm and Test Automated Key Control:**

We reviewed and recalculated automated calculations done by Pay1 for premiums as part of the premiums and assessments understanding at

# State of Washington

[Key Control #1 (Automated)] for each of the following agency groups:

Regular PEBB state agency - DSHS

SEBB - School District

PEBB Political sub-division/group - Olympia Medical Center

Retiree, no specific employer

All Pay1 calculations were accurate based on employee/employer elections. *No issues noted.*

## **Noted Weaknesses are as follows:**

none.

## **STEP 3: Understand General IT Controls**

Documentation for this general IT control is documented above in the "Controls -Pay1" step.

## **STEP 4: Confirm Key General IT Controls**

We reviewed the general control for the automated Pay1 premiums updates as part of the premiums and assessments understanding at [Key Control #1 (Automated)].

We reviewed the rate table update for PEBB composite state shares from May 2024. *No issues noted.*

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **F.4.PR.G - Due From Other Governments**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* MRF, 5/6/2024

*Reviewed By:* RKM, 6/5/2024

Purpose/Conclusion:

## **Purpose:**

## State of Washington

To confirm ERB accountants review payments automatically processed, and not automatically processed, in Pay1, and reconcile payments to AFRS daily, to ensure that revenues/receivables exist and are accurately classified for the Pay1 System (key control 2 for Pay1) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.



## State of Washington

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

## State of Washington

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #2 (Manual - Existence/Classification): Daily, ERB accountants review payments automatically processed and not automatically processed, in Pay1, and reconcile payments to AFRS to ensure that revenues/receivables exist and are accurately classified for the Pay1 System.**

The understanding for this system is documented above in the "Controls - Pay1" step.

### **1. Confirmation of Key Manual Control:**

We confirmed this control as part of Premiums and Assessments at [[Key Control #2 \(Manual\)](#)].

### **Noted Weaknesses are as follows:**

None.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

# State of Washington

## F.4.PR.G - Due From Other Governments

*Procedure Step:* Key Control #4 (Manual)

*Prepared By:* MRF, 5/6/2024

*Reviewed By:* RKM, 6/25/2024

Purpose/Conclusion:

**Purpose:**

To confirm if ERB FA4s manually adjusted receivables related to PEBB/SEBB premiums for allowance/writeoffs by journal voucher on a monthly basis (key control 4 for Pay1) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the*

## State of Washington

*person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

## State of Washington

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria.:

Record of Work Done.:

**Key Control 4 - (Valuation/Classification) Monthly, ERB FA4s manually adjusted receivables related to PEBB/SEBB premiums by journal voucher. Adjusting entries were used to record allowance for doubtful accounts and write-offs based on Pay1 report HRISD-B5519-R01 and SEBB-B5519-R01. The entry is reviewed by the FA5, ERB Accounting Section Manager, or Deputy Accounting Section Manager to ensure accuracy and classification of adjustments.**

The understanding for this system is documented above in the "Controls - Pay1" step.

### **1. Confirmation of Key Manual Control:**

We obtained the March 2024 month end receivable adjusting journal vouchers from Rita Homan, Deputy Accounting Section Manager, for PEBB and SEBB. We received a walkthrough of the process on 05/01/2024 with Rita Homan.

### **PEBB**

We obtained and reviewed the following JV:

PAJV6165 - To write off uncollectible accounts receivable to bad debt expense for March 2024 and book bad debt/uncollectible accounts receivable per aging report as of March 31, 2024, for PEBB

## State of Washington

The journal voucher was prepared on 04/04/2024 by Michael Williamson, Fiscal Analyst 4, and reviewed by Brooke Schofield, Fiscal Analyst 5 on 05/02/2024. The total amount posted was \$739,181 in a batch.

We reviewed the monthly group aging report summary HRISDB5519-R01 with run date 03/29/2024. We noted \$145,884 was in the 01-30 days column, \$274,771 was in the 31-60 days column, \$89,835 was in the 61-90 days column, \$67,975 was in the 91-120 days column, and \$60,128 was included in the "over 120" days column in the selfpay agencies group. The total aging balance per the report for self pay was \$638,593.

The balance recorded in AFRS was \$1,374,839 (excluding MODA) as of 02/29/2024 in GL 1312, Accounts Receivable. This was entered into the computational spreadsheet "pajv6165-file0002-PEBB Pay1 WO 032024" and verified by Michael Williamson.

To adjust the balance to match current aging report, a \$736,246 entry was made (\$1,374,839 less \$638,593). Entry ties to the reports noted above. **No issues noted.**

We reviewed the Write-Off Report for Month of March 2024, HRISDB5217-R01 with run date 04/01/2024. We noted the total write-off was \$869 based on accounts that were written off for various amounts. The report includes comments for why write-offs were made. The total write off amount was included in entry. Entry ties to Pay1 reports noted above. **No issues noted.**

The total of the JV was the allowance for doubtful accounts adjustment of \$736,246, the bad debt expense write off of \$869, and various corrections in the amount of \$2,065 for a total of \$739,181. **No issues noted.**

### SEBB

We obtained and reviewed the following JVs:

SAJV1482 - To book bad debt/uncollectible accounts receivable per aging report as of 03/31/2024. The journal voucher was processed 04/05/2024, prepared by Oanh Pham, Fiscal Analyst 4, and reviewed by Rita Homan, Deputy Accounting Manager. The total amount posted was \$86,931.

We reviewed the monthly group aging report summary SEBB-B5519-R01 with run date 03/29/2024. We noted \$16,321 in the 01-30 days column, \$79,033 in the 31-60 days column, \$61,802 in the 61-90 days column, \$59,696 included in the 91-120 days column, and \$45,648 in the "over 120" days column, for the selfpay agencies group. This is a total of \$262,500.

The balance recorded in AFRS was \$349,404 as of 2/29/2024 in GL 1312, Accounts Receivable, but the balance per the aging report was \$262,500. To adjust the balance to what is actually receivable per the aging report, a \$86,904 entry was made (\$349,404 less \$262,500). Entry ties to the reports noted above. **No issues noted.**

We reviewed the Write-Off Report for Month of March 2024, SEBB-B5217-R01 with run date 04/01/2024. We noted the total write-off was \$9 based on accounts that were written off for various amounts. The report includes comments for why write-offs were made. The total write off amount was included in entry. Entry ties to Pay1 reports noted above. **No issues noted.**

The JV batch entry was the \$86,904 adjusting entry for doubtful accounts, the \$9 bad debt expense write off, and an adjustment of \$18 to correct a pay1 coding error. The total on the JV was \$86,931. **No issues noted.**

### Noted Weaknesses are as follows:

None

# State of Washington

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.4.PR.G - Due From Other Governments**

*Procedure Step:* Risk Assessment

*Prepared By:* MRF, 6/26/2024

*Reviewed By:* CJG, 12/9/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

# State of Washington

## *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

## *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

## *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

## *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

## *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*



## State of Washington

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Financial Statement Audits](#) Planning Guide

Record of Work Done:

#### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Existence - **HIGH**

Valuation - **HIGH**

Classification - **HIGH**

#### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**Pay1 - MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

#### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Existence - HIGH

Valuation - HIGH

Classification - HIGH

#### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

#### **Testing to meet Existence assertion:**

## State of Washington

Obtain June 2024 month-end receivable report (summary by customer type and detail by participating employer) for both PEBB and SEBB accounts. We will use the sampling spreadsheet to select accounts to ensure the receivable existed by reviewing subsequent payments. Obtain and review a year end receivable reconciliation between Pay1 and AFRS for PEBB/SEBB to ensure amounts reported for ACFR existed.

### **Testing to meet Valuation assertion:**

Obtain June 2024 month-end receivable report (summary by customer type and detail by participating employer) for both PEBB and SEBB accounts. We will use the sampling spreadsheet to select accounts to ensure the receivable is properly calculated based on automated calculations and any adjustments. Obtain and review a year end receivable reconciliation between Pay1 and AFRS for PEBB/SEBB to ensure amounts reported for ACFR are accurate.

### **Testing to meet Classification assertion:**

Obtain June 2024 month-end receivable report (summary by customer type and detail by participating employer) for both PEBB and SEBB accounts. We will use the sampling spreadsheet to select accounts to ensure the receivable is classified properly as *due from other governments*.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **F.4.PR.G - Due From Other Governments**

*Procedure Step:* Substantive Test

*Prepared By:* MRF, 10/1/2024

*Reviewed By:* CJG, 12/9/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To determine whether reported receivables represent amounts relating to the period, were reported at properly calculated amounts and were properly classified.

### **Conclusion:**

## State of Washington

We determined receivables represent amounts relating to the period and were properly classified. We determined reported receivables were correctly calculated with the following exception:

Amounts tied to supporting documents, but some payments were incorrectly excluded from the total value of receivables as of June 30th due to timing with the July invoices. HCA agreed with the issue and conducted a review of all governments receivables to determine the true total misstatement of the Due From Other Governments receivable balance. The known misstatement of the balance is \$15,456,164.64 between both PEBB and SEBB. See issue here [[E: HCA\\_Misstatement of Due From Other Governments Receivables](#)].

We also noted the following:

PAY1 could not be fully reconciled to AFRS amounts. Due to system limitations, HCA could not track or identify variances between PAY1 and AFRS for both PEBB and SEBB. This resulted in AFRS reporting \$9,382,356 less than PAY1. See issue at [[E: HCA\\_Receivables Lack of Complete Reconciliation Pay1 to AFRS](#)].

See AOM here [[Aggregation of Misstatements \(GAAP\)](#)].

### Testing Strategy:

The following is a list of **considerations** for testing the existence assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### Receivables

- Confirm receivables with the obligated party.

- Confirm intergovernmental receivables with the other agency.

- Confirm trade receivables using negative or positive confirmations to customers. *NOTE: if trade receivables were not confirmed, auditors should document the reasons for not following the audit requirement (see policy/criteria tab).*

- Verify receivables to source billing documents, reimbursement requests or other documentation.

- If receivables are sent to an external collection agency or trigger an action that affects the obligated party (ie: water shut-off) within a reasonably short time period, trace or reconcile from the A/R Aging report to the collection agency's report or evidence of a confirming action.

- Verify receivables through subsequent receipt of funds (remittance documentation should evidence the period to which it applies).

- For the period following balance sheet date, scan the accounts receivable general ledger control account for material charge-off and unusual transactions, and investigate.

Perform analytical procedures to determine the reasonableness of receivable balances and follow-up on any unexpected results. For example, trend analysis of aged A/R, trend of beginning balance, billings, adjustments, payments and ending balance, inventory/volume usage

## State of Washington

reconciliation, etc.

The following is a list of **considerations** for testing the valuation assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Review the entity's calculation of the value of intangible assets.

Review the entity's calculation of write-off of inventory or other assets due to obsolescence or damage.

### **Calculation or Realizable Value of Receivables**

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

The following is a list of **considerations** for testing the classification assertion for other assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Classification as Current or Non-Current**

If any amounts are noted through testing that will not be collected within one year, ensure they are reported as a non-current account receivable (must use classified format per GASB 34 paragraph 97). For example, a patient balance of \$100,000 and the patient has a repayment agreement to make \$50 per month payments or established a history of small payments that would allow the District to reasonably determine that the amount will not be collected within one year.

### **Classification between Opinion Units**

Search for manual journal entries that transfer other assets from one opinion unit to another without recording an operating statement transaction (debit and credit to capital assets and fund balance for each opinion unit, respectively). Consider testing if any risk indicators are noted.

Evaluate whether receivables or other assets appear reasonable in relation to the activities of the fund. Follow-up on any unexpected results.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6350](#) – External Confirmations**

# State of Washington

## **Purpose:**

To determine whether other assets were reported at properly valued or calculated amounts.

## **Current & Non-Current (Government-wide and Proprietary Statements)**

GASB 34 paragraph 31 defines "current" and "non-current" classification of assets:

"Governments are encouraged to present assets and liabilities in order of their relative liquidity. An asset's liquidity should be determined by how readily it is expected to be converted to cash and whether restrictions limit the government's ability to use the resources. A liability's liquidity is based on its maturity, or when cash is expected to be used to liquidate it. The liquidity of an asset or liability may be determined by assessing the average liquidity of the class of assets or liabilities to which it belongs, even though individual balances may be significantly more or less liquid than others in the same class and some items may have both current and long-term elements ..."

Record of Work Done:

## **Sampling Methodology:**

We obtained PAY1 PEBB (HRISDB5381-R01) and SEBB (SEBBB5381-R01) receivable reports from HCA for June 30, 2024. We converted receivable reports from txt files to Excel using text to columns. We used the sampling spreadsheet in accordance with SAO sampling policy 3240 to determine our sample size for amounts due from other governments for both SEBB and PEBB.

## **SEBB (School Employees) [SEBB Due From Other Governments FS Sampling]:**

We randomly selected transactions using the small population method per the sampling spreadsheet. We determined the random sample seemed a reasonable representation of our population.

## **PEBB (Political Sub-div) [PEBB Due From Other Governments FS Sampling]:**

We initially randomly selected transactions per the sampling spreadsheet, but noted the average dollar amount of the testing population was significantly smaller than the average of the total population. We met with Jordan Prince, Sampling Specialist, on 8/19/2024 to discuss the best methodology to sample. We determined the following:

- We are unable to perform stratification of selections because the data set is too small and "bottom heavy" (a few very large items).

- Per the sampling spreadsheet, we should select 14 transactions. We would have to select the top 14 transactions to get 90% coverage, which is not an accurate representation of our population.

- Selections with a total dollar amount under \$1,000 should not be included in our sample selection population. The total of these items is less than 0.025% of the total population and any issues would be insignificant.

- We would judgmentally select amounts over \$400k and include them in the individually significant items (ISI), for a total of five ISIs.

- We would randomly select transactions through the remaining population, excluding the small amounts and the judgementally selected ISIs.

# State of Washington

## **Substantive tests performed to meet the Existence / Occurrence assertion:**

We obtained the June 2024 month-end receivable report (summary by customer type and detail by participating employer) for both PEBB and SEBB accounts. We selected accounts using approved sampling methodology to ensure the receivable existed by reviewing subsequent payments.

We reviewed invoices for June 30, 2024 (invoiced in May) for all selected employers and any subsequent payments for the invoices (warrants, deposit slips, ACH support, images from US Bank lockbox data) to ensure the receivable existed at year end. We tied actual invoice amounts to the B5381 report and INV-PMT, an invoice payment history provided by HCA. See testing performed in the "PEBB Population Testing" and "SEBB Population Testing" tabs. *No issues noted.*

We obtained and reviewed the year end receivable reconciliation between Pay1 and AFRS for PEBB/SEBB to ensure amounts reported for ACFR existed.

We obtained a reconciliation performed by Rita Homan, HCA Deputy Accounting Section Manager, for both PEBB and SEBB to AFRS. See tabs "PEBB Reconciliation" and "SEBB Reconciliation" in each of the testing spreadsheets. HCA used the month end receivable report (B5381) reduced by the following to tie amounts to AFRS:

- employer prepayments

- employee receivable report amounts not included in B5381 (from report B5519) and prepayments

- US Bank Lockbox receipts recorded in AFRS (not in B5381)

HCA identified the following variances that could not be determined due to lack of supporting reports from PAY1:

- PEBB - \$2,039,922 more reported in PAY1 reports

- SEBB - \$7,342,434 more reported by PAY1 reports

See issue related to HCA's PAY1 reconciliations at [[E: HCA\\_Receivables Lack of Complete Reconciliation Pay1 to AFRS](#)]. The variance is above the floor, we will carry this issue to the aggregation of misstatements [[Aggregation of Misstatements \(GAAP\)](#)].

## **Substantive tests performed to meet the Valuation assertion:**

We used the selected sample of accounts and tested to ensure the receivable is properly calculated based on automated calculations and any adjustments.

We recalculated the amount due (receivable) as of June 30, 2024. We recalculated by taking the amount of the invoices for June 30, 2024 (invoiced in May) and adding any remaining balance forward from previous periods (report HRISDB5079-R01), less any payment(s) received by the government for coverage provided before June 30th, 2024. We compared the recalculated amount to PAY1 and INV-PMT. See tabs "PEBB Reconciliation" and "SEBB Reconciliation" in each of the testing spreadsheets.

We identified variances in both PEBB and SEBB testing for the valuation of the receivables. We noted the variances matched the June payment amounts exactly and followed up with Rita Homan of HCA. We determined the error was due to the following:

- PAY1 report 5381 (group aging summary report) excludes payments made after invoicing runs for the following month. Payments are recorded in PAY1 for the subsequent coverage month, but are recorded accurately in AFRS as payment for the current month.

## State of Washington

The 5381 report excludes payments posted after the invoicing cycle for each program (different invoice cycles), causing an overstatement of the receivable balance at the end of each month.

Using the sampling spreadsheet, we estimated the total error was between \$300k and \$44M based on if the issue is found in small or large payments.

Rita Homan performed follow up work and reviewed all Other Government's receivable balances that had payments after July invoicing. HCA determined the true misstatement of the balance was \$15,456,164.64 between both PEBB and SEBB. Rita Homan provided the billing reports as excel sheets detailing the calculated balance of the receivable and screenshots of the Pay1 report 5381 aging reports to show that the June payments were incorrectly excluded from the total receivables. We reviewed the supporting material provided by Rita Homan and agreed with the calculations, and since the error was found in a mix of primarily smaller payments with a few large payments, we determined the amount of \$15.5M is reasonable. See issue here [[E: HCA Misstatement of Due From Other Governments Receivables](#)]. The variance is above the floor, we will carry this issue to the aggregation of misstatements [[Aggregation of Misstatements \(GAAP\)](#)].

### **Substantive tests performed to meet the Classification assertion:**

We obtained the June 2024 month-end receivable report (summary by customer type and detail by participating employer) for both PEBB and SEBB accounts. We reviewed the government types for the PEBB population and noted they were all listed as political subdivisions or education, we noted no state agencies.

For the randomly selected samples, we reviewed invoices for June 30, 2024 (invoiced in May) for all selected employers and any subsequent payments for the invoices (warrants, deposit slips, ACH support, images from US Bank lockbox data) to ensure the receivable was classified properly as due from other governments. We ensured invoices were processed for actual governments (non-federal) and were for the correct period (expected to be collected within one year). All invoices were for the coverage period of 6/30/2024 for actual governments. See testing performed in the "PEBB Population Testing" tab. ***No issues noted.***

### **F.5.PRG - Receivables**

*Procedure Step:* Summary & Conclusion

*Prepared By:* MRF, 9/30/2024

*Reviewed By:* RKM, 11/24/2024

Purpose/Conclusion:

### **Purpose:**



# State of Washington

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

## **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

## **Information to be used as audit evidence:**

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

## State of Washington

Is information precise enough to catch if misstatements exceeded the tolerable level?  
Is information detailed enough to conclude on whether or not there were misstatements?  
Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?  
How did misstatements occur and how often might they occur again in the population?  
Were misstatements caused by control deficiencies or circumvention of controls?  
If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?  
If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.  
Did tests identify a different level or type of risk than the planned audit response was designed to address?  
If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done.:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

# State of Washington

## **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

## **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **F.5.PRG - Receivables**

*Procedure Step:* Understanding of Line Item

*Prepared By:* MRF, 5/22/2024

*Reviewed By:* RKM, 6/5/2024

Purpose/Conclusion:

#### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

#### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

#### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

## State of Washington

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.7

# State of Washington

Record of Work Done:

## **(1) Prior Audit Exceptions:**

During FY23 we found that HCA has no documented process in place to review the accuracy of claims data provided to Milliman and relies on Milliman's procedures alone to determine the receivables balance.

We inquired with Sara Whitley, ERB Finance Manager, about this prior audit issue on April 26, 2024, and she informed us that there's sections of HIPPA that restrict the "plan sponsor" (HCA) from reviewing claims data passed directly from "group health plans" (third party administrators [TPA]). Specifically, these sections are [45 CFR 164.504, sections f\(2\) and \(3\)](#). Sara stated that the Authority contracts with Milliman to check for reasonableness of the raw claims data, that the Authority depends on TPAs to provide accurate claims data to Milliman, and as a compensating control, HCA compares claims reports from TPAs and compares the amounts in those reports to prior period amounts to ensure that trends are aligning with the Authority's expectations (see our control understanding and the confirmation work we did for key control #1 for more details on this last item). Considering that HCA is not allowed to review the claims data in detail, per HIPPA, and considering HCA's compensating control of reviewing TPA reports to ensure the claims amounts align with HCA's expectations, we've determined that it's reasonable for HCA to not review key claims data in detail. **No issues noted.**

## **(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

Receivables at year end consist of two categories: Normal operational receivables and year end adjustments/specialty amounts.

Normal operational receivables, include insurance premiums billed but not paid, to two main groups.

1. Active Employees - State and Local
2. COBRA/Self Pay - State and Local- Per inquiry with HCA, Fund 721 receivables consist of receivables that stem from premiums billed to PEBB self-pay retirees/COBRA.

Local government receivables (GL 1352) are reported in the "due from other governments" line item and do not need their work replicated here. State government receivables (GL 1354) is a very small balance and is not expected to be material to any of the line items. *As such, normal operational receivables will not be covered in the receivables balance testing.*

Year end Adjustments/specialty amounts include two categories:

1. MODA pharmaceutical rebates - **Fund 721** - Public Employees' and Retirees Insurance Account

In the prior year, rebate receivables from MODA Health for pharmaceutical were also reported as a receivable in Fund 721. HCA's contracted actuary, Milliman, provided a memo in February 2023 that changed the reporting for MODA rebate receivables and they are now reported

## State of Washington

in IBNR update quarterly. *We do not expect MODA rebate receivables to affect the receivables balance and will not be included in our control understanding or substantive testing.*

### 2. SEBB risk rate adjustments - **Fund 493** - School Employees' Insurance Account

Per inquiry with HCA, Fund 493 receivables consist of a SEBB Risk adjustment Transfer and receivables that stem from premiums billed to SEBB self-pay retirees/COBRA. HCA expects the majority of the receivables balance to be a result of the SEBB risk rate adjustment transfer.

### **(3) Updates to Significant Account Matrix:**

We made no changes to the Significant Account Matrix.

### **F.5.PRG - Receivables**

*Procedure Step:* Controls - Milliman Calculation

*Prepared By:* MRF, 5/22/2024

*Reviewed By:* RKM, 6/5/2024

Purpose/Conclusion:

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

#### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant

## State of Washington

assertion(s), and note any control weaknesses.

In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

Who or what initiates the control

When (or how often) is the control applied

Who performs the control

As needed, the experience, knowledge and attitude of the person applying the control

## State of Washington

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any exceptions or alternative processing to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**



# State of Washington

## Financial Statement Audits Planning Guide

Record of Work Done:

### **Material Balance(s) and Assertions**

Internal controls in the Milliman Calculation address the following balance(s):

#### **Receivables**

For the following assertions:

**Valuation** - There is a risk that: risk adjustments, supporting receivables from managed care plans, may not be supported by amounts determined by actuaries; HCA used actuaries that were not creditable or lacked experience (educational and professional) to determine estimate; assumptions based on unaudited attestations made by HCA were not accurate (i.e. information relied on by Milliman did not reflect actual operations or benefits provided); and claim history information provided to Milliman was not complete (i.e. multiple sources of claims).

### **Gain an Understanding of Internal Controls**

We met with HCA staff on 05/02/2024 to review controls over accounts receivable for GL 1312. We met with the following staff:

Rita Homan, HCA Assistant Accounting Section Manager  
Kari Summerour, HCA Liaison  
William Sogge, HCA Liaison  
Sara Whitley, ERB (Employee Benefits Board both PEBB and SEBB) Finance Unit Manager  
Lisa Kolle, ERB Accounting Manager (Started in March 2024)  
Samantha Zimmerman, Internal Controls Officer (Started in Feb 2024)

### **Background**

We noted receivables in GL 1312 were recorded in the following funds:

Fund 721 - Public Employees' and Retirees Insurance Account  
Fund 493 - School Employees' Insurance Account

Receivables included in these funds were a result of Public Employees Benefit Board (PEBB) and School Employees Benefits Board (SEBB) insurance premiums billed and not yet paid. These billings are recorded 2 different ways depending on the party being billed:

Active employees - This includes state agency, higher education, and K12 active employees. The employer is billed as part of the invoicing cycle and pays HCA. Since the accounts receivable are due from state/local governments, these amounts are reported in GL 1352, due from other governments. See our understanding of due from other governments at [[Understanding of Line Item](#)].

## State of Washington

COBRA (Consolidated Omnibus Budget Reconciliation Act) continuing coverage/retirees self-pay - This includes amounts invoiced but not paid from retirees and COBRA participants. These receivables are included GL 1312, accounts receivables, and are the individuals responsibility to pay. These historically represent a small portion of the total receivables balance. We do not expect the COBRA receivables to make up a significant portion of the Receivables balance.

Receivables include significant adjustments in fund 493 to record the SEBB risk rate adjustment. Based on our understanding of the line item at [\[Understanding of Line Item\]](#), we noted a majority of the Receivables balance is expected to be the SEBB risk rate adjustment. In the prior year, the SEBB risk rate adjustment made up 70% of the balance. Without the adjustment related to MODA rebate receivables, the SEBB risk adjustment is expected to represent a larger portion of the receivables balance. As such, we determined focusing our understanding and substantive testing on SEBB risk rate adjustment alone will provide sufficient coverage of the Receivables balance.

### **SEBB Risk Rate Adjustment Transfer**

Rita explained the SEBB risk rate adjustment is done at year end to adjust for the difference from the expected rate used in the plan calculations to the actual rate at year end. Since SEBB is relatively new, she expects this rate adjustment will continue being made for the next few fiscal years. As the plan goes on, Rita expects the differences to be less between expectations and actual. This process is similar to how PEBB was treated when it was first implemented. HCA contracts with Milliman to calculate the final risk adjustment transfer payments for each carrier that is participating in the School Employees Benefits Board (SEBB) health insurance program. The participating carriers in the SEBB program included Uniform Medical Plans (UMP), managed care organizations (MCOs) of Kaiser Permanente of Washington (KPWA), Kaiser Permanente of Washington Options (KPWAO), Kaiser Permanente Northwest (KPNW), and Premera. Milliman does this risk adjustment once a year in August to ensure all activity as of June 30 is included.

### **SEBB Claims Data**

Milliman works with the Employee Retiree Benefits (ERB) Finance division as the main contact within HCA. Per Sara Whitley, ERB Finance Unit Manager, Milliman's calculation for the SEBB risk adjustment transfer uses claims incurred between 1/1/23 and 12/31/23 and paid between 1/1/23 and 3/31/24. Milliman receives raw claims data directly from Regence (UMP) and the fully insured carriers (Kaiser Permanente/Premera) which includes all medical claims data, pharmacy claims data, and membership diagnosis codes for the time period. HCA establishes contracts with each of the insured carriers and requirements related to when and what data is to be provided for the Risk adjustment transfer, as detailed in the contract under the Risk Adjustment Exhibit. The terms related to risk adjustment are standardized for all contracts to ensure processes and data submitted to Milliman is uniform for their processing. On a quarterly basis, ERB will meet with the contracted carriers and discuss general plan management topics. As part of the meetings, the carriers present reports that compare what carriers are submitting to Milliman in relation to raw claims and what the carriers have on record for those amounts.

Once the data is received by Milliman, the data is processed through the Milliman Advanced Risk Adjustment (MARA) software to refresh risk scores used in the calculation of the risk adjustment transfer. Milliman has their own separate analytical procedures to ensure claims data received is accurate, complete, and reasonable. Using historical data available to them, Milliman confirms the following:

## State of Washington

Distribution of claim counts by month for each carrier is relatively reasonable based on expectations. This review looks for possible over or under reporting within a single month for any of the carriers. The expectation is that the number of claims in a month is proportional to the workdays within the month.

Paid runout is consistent with historical data. This review looks for possible changes in processing patterns that may lead to inconsistent reporting speeds within the data. The expectation is that the processing of runout is consistent with historical observations and that there is neither a buildup or expansion of backlog that may influence the reported data.

Diagnosis code positions are populated as they would expect. The expectation of diagnosis code positions is based on historical data where consistency of reporting is evaluated based on the count of diagnosis code positions included within the data.

The number of invalid members or orphaned claims (i.e. claims that cannot be matched with an enrollment record) are limited and in line with historical expectations. The data used in the process of risk adjustment requires that HCA reports the member as eligible for funding, and that the carrier reports diagnosis codes that are matched with the enrollment record. Milliman determines a reasonable match rate based on their experience with other risk adjustment data sets.

Since raw claims data is heavily protected under HIPPA compliance rules, HCA has limited access to data from third party administrators (Regence) and fully insured carriers. HCA relies on Milliman's analysis and review of the raw claims data to ensure information is accurate and complete. HCA's ERB unit also utilizes comparison tools to perform high level reviews of Milliman's raw feed and the information reported in their memos/other deliverables, including the risk adjustment memo. Although HCA cannot perform a review of raw claims data, they have the following processes to ensure reasonableness of data provided to Milliman:

On a quarterly and annual basis, HCA meets with the carriers to discuss general plan management topics and utilization. The reports supplied during these quarterly meetings are created by the carriers and allow a point of comparison between what the carriers are submitting to Milliman with respect to raw claims, and what the carriers have on record for these amounts.

Each year during rate development HCA uses the completed "Bid Rate Forms" to verify information supplied to Milliman is generally aligned with carrier inputs of information (to include claims by category of service, trends, actuarial memorandums, etc.).

### **Adjustment Calculation**

The Milliman memo details the amount due from/owed to each carrier. All underlying assumptions, analysis of claims data, and methodology are documented within Milliman's memo related to the Risk Adjustment Transfer. Upon receipt of the Milliman calculation, the ERB Finance team performs a review of the calculation for reasonableness and will follow up on significant changes with Milliman. As the contact within HCA, ERB also meets weekly with Milliman during the preparation of the risk adjustment calculation to ensure the calculations appear reasonable with previous year interim analysis. HCA relies on actuary work performed by Milliman for the calculation of the SEBB Risk Rate Adjustment to ensure SEBB receivables are accurately valued for the ACFR (**Key Controls #1 - Valuation**).

### **Year End Adjusting Entry**

HCA uses their excel workbook SEBB Risk Adjustment Transfer to track payments receivable and reconcile that information to the Milliman memo. The workbook show receivables outstanding as of year end. The JV at year end for the SEBB Risk Adjustment Transfer is prepared by an FA and

## State of Washington

reviewed by Rita Homan, Accounting Section Manager, to ensure the entry is accurate and supported by Milliman's calculations (**Key Control #1 - Valuation**).

### How Transactions are Recorded in AFRS:

SEBB Risk Rate Adjustment Transfer - ERB Accountants prepare a journal voucher to record receivables identified by Milliman at year end.

### Key Controls are as follows:

Key Control #1 (Valuation) - HCA relies on actuary work performed by Milliman for the calculation of the SEBB Risk Rate Adjustment to ensure SEBB receivables are accurately valued for the ACFR. At year end, a Fiscal Analyst from the accounting section prepares the SEBB Risk Adjustment Transfer JV and the Accounting Section Manager reviews the entry to ensure the amount is accurate and supported by Milliman's Calculations.

### Noted Weaknesses are as Follows:

None.

### F.5.PR.G - Receivables

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* EZM, 9/23/2024

*Reviewed By:* RKM, 9/26/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm Fiscal Analyst prepares the SEBB Risk Adjustment Transfer based on actuarial calculations performed by Milliman (Key Control 1 for AFRS) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess**

## State of Washington

**control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be***

## State of Washington

*reported as findings.*

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control 1- Valuation:** HCA relies on actuary work performed by Milliman for the calculation of the SEBB Risk Rate Adjustment to ensure SEBB receivables are accurately valued for the ACFR. At year end, a Fiscal Analyst from the accounting section prepares the SEBB Risk Adjustment Transfer JV and the Accounting Section Manager reviews the entry to ensure the amount is accurate and supported by Milliman's Calculations.

The understanding for this system is documented above in the "Controls - Milliman Calculation" step.  
We recieved the Milliman memo on September 20, 2024.

### **1. Confirmation of Key Manual Control:**

We received JV SAJV1600 from Rita Homan, Accounting Section Manager. We noted it was prepared by Katherine Plaquet, Fiscal Analyst 5, on 8/27/2024 and reviewed/approved by Rita Homan, Accounting Section Manager, on 8/27/2024. We noted the total amount to the risk adjustment accruals was \$94,981,952. The entry was broken down into the following: Table 1 2023 Final Risk Adjustment Transfer Overview- Paid through March 2024 Processing Period.

Kaiser Foundation Health Plan of WA (KPWA): -\$50,294,274  
Kaiser Foundation Health Plan of WA Options (KPWAO): \$28,640,705  
Kaiser Foundation Health Plan of the Northwest (KPNW): -\$9,868,009  
Premera: -\$6,178,964

We reviewed the HCA prepared workbook "Accounting\_SEBB 2023 Net Transfer Payment Tables" and all amounts from the entry tied without exception. The workbook was calculated based on actuarial calculations from Milliman and the entry ties to Milliman calculations without exception. See the Milliman memo dated August 30, 2024 at [[Final 2023 SEBB Risk Transfer Report](#)]. To determine if we can rely on the work of Milliman, we performed the rely on specialist step at [[Rely on Work of Specialist](#)].

### **Noted Weaknesses are as follows:**

None.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be

# State of Washington

effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **F.5.PR.G - Receivables**

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* EZM, 9/23/2024

*Reviewed By:* RKM, 9/26/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm Fiscal Analyst prepares the SEBB Risk Adjustment Transfer based on actuarial calculations performed by Milliman (Key Control 1 for AFRS) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals*



## State of Washington

*ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

## State of Washington

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 1- Valuation:** HCA relies on actuary work performed by Milliman for the calculation of the SEBB Risk Rate Adjustment to ensure SEBB receivables are accurately valued for the ACFR. At year end, a Fiscal Analyst from the accounting section prepares the SEBB Risk Adjustment Transfer JV and the Accounting Section Manager reviews the entry to ensure the amount is accurate and supported by Milliman's Calculations.

# State of Washington

The understanding for this system is documented above in the "Controls - Milliman Calculation" step.  
We recieved the Milliman memo on September 20, 2024.

## **1. Confirmation of Key Manual Control:**

We received JV SAJV1600 from Rita Homan, Accounting Section Manager. We noted it was prepared by Katherine Plaquet, Fiscal Analyst 5, on 8/27/2024 and reviewed/approved by Rita Homan, Accounting Section Manager, on 8/27/2024. We noted the total amount to the risk adjustment accruals was \$94,981,952. The entry was broken down into the following: Table 1 2023 Final Risk Adjustment Transfer Overview- Paid through March 2024 Processing Period.

Kaiser Foundation Health Plan of WA (KPWA): -\$50,294,274

Kaiser Foundation Health Plan of WA Options (KPWAO): \$28,640,705

Kaiser Foundation Health Plan of the Northwest (KPNW): -\$9,868,009

Premiera: -\$6,178,964

We reviewed the HCA prepared workbook "Accounting\_SEBB 2023 Net Transfer Payment Tables" and all amounts from the entry tied without exception. The workbook was calculated based on actuarial calculations from Milliman and the entry ties to Milliman calculations without exception. See the Milliman memo dated August 30, 2024 at [[Final 2023 SEBB Risk Transfer Report](#)]. To determine if we can rely on the work of Milliman, we performed the rely on specialist step at [[Rely on Work of Specialist](#)].

## **Noted Weaknesses are as follows:**

None.

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.5.PR.G - Receivables**

*Procedure Step:* Risk Assessment

*Prepared By:* MRF, 6/18/2024

# State of Washington

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

*General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

*Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

## State of Washington

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

## State of Washington

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation – **HIGH**

#### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**AFRS – MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

#### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation – HIGH

# State of Washington

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

Obtain June 2023 Risk Adjustment Transfer Memo (for FY 24) from Milliman and tie to HCAs workbook and entry to ensure amounts reported to AFRS are supported by actuarial calculation.

Perform rely on work of others - specialist step (obtained from TeamStore) for Milliman to determine the actuary is creditable and experienced to perform the calculation of SEBB Risk Adjustment for receivables.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## **F.5.PRG - Receivables**

*Procedure Step:* Substantive Test

*Prepared By:* EZM, 9/20/2024

*Reviewed By:* RKM, 10/2/2024

Purpose/Conclusion.:

### **Purpose:**

To determine whether receivables were reported at properly calculated amounts.

### **Conclusion:**

We determined receivables were reported at properly calculated amounts.

Testing Strategy.:

Guidance/Criteria.:

## State of Washington

Record of Work Done:

### **Substantive tests performed to meet the Valuation assertion:**

#### Testing Procedures:

We obtained the June 2023 Risk Adjustment Transfer Memo (for FY24) from Milliman and tied to HCAs workbook and entry to ensure amounts reported to AFRS are supported by actuarial calculation.

We performed the rely on work of others - specialist step (obtained from teamstore) for Milliman to determine the actuary is creditable and experienced to perform the calculation of SEBB Risk Adjustment for receivables.

#### Testing Results:

The SEBB fund 493 covers 99.2% of the total receivables balance based on our breakdown in the lead sheet [[Line Item Lead Sheet](#)]. We noted that the SEBB Risk Adjustment Transfer alone makes up 99.3% of the SEBB fund 493 Receivables balance. See [[SEBB Risk Adjustment Transfer Testing](#)]. We considered this review to provide sufficient coverage of the total receivables balance reported in the health insurance fund. ***No issues noted.***

We obtained the Milliman Memo for the June 2023 Risk Adjustment Transfer [[Final 2023 SEBB Risk Transfer Report](#)] from Sara Whitley, Employee Retiree Benefits Finance Unit Manager. We obtained HCA's year end journal entry, SAJV1600, from Rita Homan, HCA Assistant Accounting Section Manager. We tied amounts directly from HCA's year end entry for each carrier to Milliman's calculation without exception. All reported receivable amounts from carriers were supported by Milliman calculation. See review at [[SEBB Risk Adjustment Transfer Testing](#)]. ***No issues noted.***

We performed a review of specialist work by Milliman to ensure we could rely on their work as part of substantive testing. Based on our review of the specialist's competence, capability, objectivity, and our understanding/evaluation of specialist's work and conclusions, we determined we can rely on Milliman's work. See [[Rely on Work of Specialist](#)]. ***No issues noted.***

### **F.6.PRG - Accounts Payable**

*Procedure Step:* Summary & Conclusion

*Prepared By:* EZM, 10/9/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:



# State of Washington

## **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

## **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### **Information to be used as audit evidence:**

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

## State of Washington

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

Is information precise enough to catch if misstatements exceeded the tolerable level?

Is information detailed enough to conclude on whether or not there were misstatements?

Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?

How did misstatements occur and how often might they occur again in the population?

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

# State of Washington

## Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

**(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

No, the results of substantive tests do not indicate a need to modify our risk assessment.

**(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

Yes, the quality and quantity of evidence obtained was sufficient and appropriate.

## F.6.PRG - Accounts Payable

*Procedure Step:* Understanding of Line Item

*Prepared By:* EZM, 6/5/2024

*Reviewed By:* RKM, 6/7/2024

## Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

## State of Washington

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

# State of Washington

Guidance/Criteria:

Record of Work Done:

**(1) Prior Audit Exceptions:**

None.

**(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

This line item is the total of all GL 5111 balances in the PEBB and SEBB program funds, including administrative funds for the programs. Activity in this line item is for June or prior services (related to the Premiums and Claims line item) that will be paid after fiscal year end (typically in July or August).

*ACFR Database*

We performed an analysis to review the composition of this ACFR line item. See [\[Line Item Lead Sheet\]](#) for details.

We analyzed the payable amounts in the line item lead sheet and identified funds 493 (SEBB) and 721 (PEBB) as the significant funds for this line item. We also noted that the FY23 fund percentage compositions were in line with FY22 with the exception of funds 493 and 721 which each had changes of approximately 22%. Fund 493 decreased from the prior year by 22.36% and fund 721 increased by 22.24%.

We noted that this balance has doubled from FY22. Per Rita Homan, Deputy Accounting Section Manager, this is due to the timing of payments and the cut-off period. There were payments to Regence and Delta Dental that would normally be paid prior to the cut-off that had to be accrued.

**(3) Updates to Significant Account Matrix:**

None.

**F.6.PRG - Accounts Payable**

*Procedure Step:* Controls - AFRS

*Prepared By:* EZM, 4/30/2024

# State of Washington

*Reviewed By:* RKM, 9/11/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

## State of Washington

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

# State of Washington

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Material Balance(s) and Assertions**

Internal controls in AFRS address the following balance(s):

Accounts Payable

For the following assertions:

Valuation - There is a risk that PEBB/SEBB premiums & claims services accrued to accounts payable are not adequately supported by invoices or weekly claims requests. There is a risk that these accruals are not properly valued (e.g. the amount accrued does not correspond with the invoiced amount).

## **Gain an Understanding of Internal Controls**

We met with Rita Homan, Deputy Accounting Section Manager, and Lisa Kolle, PEB Accounting Manager, on April 18, 2024, to gain an



## State of Washington

understanding of the controls over Accounts Payable.

Every month, HCA receives invoices from third party administrators (TPA) including MODA, Regence, and Delta Dental) which are sent to a shared accounts payable inbox directly by the TPAs. A Fiscal Analyst 3 or 4 will review the invoices and run a report from the claims SQL database for the specific date range of the invoice. If the claims data report and invoice amounts do not tie for a particular TPA, the Fiscal Analyst will contact the internal HCA account manager of that TPA and will work with them to reconcile the difference. When the claims detail and invoice tie, the Fiscal Analyst reaches out to the internal HCA account manager to get their approval to pay and once they offer their approval, the Fiscal Analyst prepares the A19 and the SQL claims report to support the payment accrual. The Fiscal Analyst enters the transaction into AFRS and uploads documentation (A19, SQL claims report, invoice) into WebAX (HCA's digital documentation system) for review. Katherine Plaquet, Fiscal Analyst 5, reviews and releases the transaction in AFRS. The Fiscal Analyst 5 reviews the transaction to ensure they are supported by appropriate documentation and that coding and amounts are accurate.

At the end of every month, a Fiscal Analyst 4 performs GL 5111 reconciliation for many of the funds associated with this GL. Reconciliations are performed on funds 418, 439, 492, 493, 494, and 721 as these are the funds with the most activity. The dental admin funds (438 and 475) only have one payment each month and are not reconciled with an official reconciliation document. The Fiscal Analyst performs the reconciliation using an "Outstanding Balance Detail" report to ensure that the vendors being paid are expected, transactions are properly clearing the GL, and transactions are coded and valued correctly. Once complete, they will email the reconciliation to Katherine Plaquet, Fiscal Analyst 5, for secondary review to ensure the accounts payable balance is valued correctly (**Key Control #1 - Valuation**).

### **How Transactions are Recorded in AFRS:**

The Fiscal Analyst enters the transaction into AFRS and uploads data into WebAX. A Fiscal Analyst 5 reviews and releases the transactions into AFRS.

### **Key Controls are as Follows:**

**Key Control #1 - (Valuation - Manual)** - At the end of every month, a Fiscal Analyst performs the GL 5111 reconciliations using an "Outstanding Balance Detail" report to ensure that the vendors being paid are expected, transactions are properly clearing the GL, and transactions are coded and valued correctly. Once complete, the Fiscal Analyst will email the reconciliation to a Fiscal Analyst 5 for secondary review to ensure the accounts payable balance is valued correctly.

### **Noted Weaknesses are as Follows:**

None.

### **F.6.PR.G - Accounts Payable**

# State of Washington

*Procedure Step:* Key Control #1 (Manual)  
*Prepared By:* EZM, 5/15/2024  
*Reviewed By:* RKM, 7/5/2024

## Purpose/Conclusion:

### **Purpose:**

To confirm that at the end of every month, a Fiscal Analyst performs the GL 5111 reconciliations using an "Outstanding Balance Detail" report to ensure that the vendors being paid are expected, transactions are properly clearing the GL, and transactions are coded and valued correctly, and that a Fiscal Analyst 5 then performs a secondary review of this reconciliation (**Key Control #1 for AFRS**) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls. However, we noted the following insignificant control deficiency:

HCA staff did not prepare or review the November 2023 GL 5111 reconciliations in a timely manner. Per our control understanding, Fiscal Analysts are supposed to perform these reconciliations at the end of every month, but the PEBB GL 5111 November 2023 reconciliation wasn't performed until the end of January 2024, and the SEBB GL5111 November 2023 reconciliation wasn't performed until March 2024. When we inquired with Rita Homan, Deputy Accounting Section Manager, about this, she informed us that HCA tries to perform these reconciliations on a monthly basis, but they weren't able to during this fiscal year due to being short staffed. **See issue: [V: HCA Accounts Payable Reconciliations Were Not Performed Timely]**

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has*

## State of Washington

*been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional*

## State of Washington

*testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 1 (Valuation):** At the end of every month, a Fiscal Analyst performs the GL 5111 reconciliations using an "Outstanding Balance Detail" report to ensure that the vendors being paid are expected, transactions are properly clearing the GL, and transactions are coded and valued correctly. Once complete, the Fiscal Analyst will email the reconciliation to a Fiscal Analyst 5 for secondary review to ensure the accounts

# State of Washington

payable balance is valued correctly.

The understanding for this system is documented above in the "Controls - AFRS" step.

## **1. Confirmation of Key Manual Control:**

Rita Homan, Deputy Accounting Section Manager, provided the fund 493 (SEBB) and fund 721 (PEBB) fiscal month 05 (November 2023) reconciliations.

**PEBB** - We reviewed the FM05 GL 5111 reconciliation for fund 721 and noted that the reconciliation was created by Michael Williamson, Fiscal Analyst, on 1/31/2024 and was reviewed and approved by Katherine Plaquet, Fiscal Analyst 5, on 1/31/2024. We also reviewed the "Download by Vendor" tab in the excel spreadsheet, which serves as the the "Outstanding Balance Detail" report, which detailed the amount owed to each vendor, the transaction code used, and the total amount payable for fund 493 as of 11/30/2023. We noted that the following transaction codes were used to account for GL 5111:

- 198 - Refund Recorded as Revenue (TREA)
- 210 - Record Account/Voucher Payable - No Encumbrance (TREA)
- 390 - Pay Revenue Account/Voucher Payable - No Encumbrance (TREA)
- 397 - Pay Account/Voucher Payable (TREA)
- 398 - Pay Expenditure Account/Voucher Payable (TREA)
- 736 - Record Account/Voucher Payable - No Encumbrance
- 955 - Request Warrant
- 956 - N/ALL\_PAY\_ACCRUED\_CONTRACTS\_PAYABLE

We inspected the [Transaction Code Table spreadsheet from OFM's website](#) and we noted that each of these transaction codes feed into GL 5111, and as such, we've determined that these accounts payable transactions were properly recorded. The final balance of (\$30,817,968.09.18) on the reconciliation ties to the November 2023 fund 721 GL break down tab and the outstanding balance detail tab without exception.

**SEBB** - We reviewed the FM05 GL 5111 reconciliation for fund 493 and noted that the reconciliation was created by Oanh Pham, Fiscal Analyst, on 3/19/2024 and was reviewed and approved by Katherine Plaquet, Fiscal Analyst 5, on 3/19/2024. We also reviewed the "Download by Vendor" tab in the excel spreadsheet, which serves as the the "Outstanding Balance Detail" report, which detailed the amount owed to each vendor, the transaction code used, and the total amount payable for fund 493 as of 11/30/2023. We noted that the following transaction codes were used to account for GL 5111:

- 198 - Refund Recorded as Revenue (TREA)
- 210 - Record Account/Voucher Payable - No Encumbrance (TREA)
- 390 - Pay Revenue Account/Voucher Payable - No Encumbrance (TREA)
- 397 - Pay Account/Voucher Payable (TREA)

# State of Washington

398 - Pay Expenditure Account/Voucher Payable (TREA)  
736 - Record Account/Voucher Payable - No Encumbrance  
955 - Request Warrant  
956 - N/ALL\_PAY\_ACCRUED\_CONTRACTS\_PAYABLE

We inspected the [Transaction Code Table spreadsheet from OFM's website](#) and we noted that each of these transaction codes feed into GL 5111, and as such, we've determined that these accounts payable transactions were properly recorded. The final balance of (\$12,600,986.91) on the reconciliation ties to the November 2023 fund 493 GL break down tab and the outstanding balance detail tab with no exceptions.

## **Noted Weaknesses are as follows:**

HCA staff did not prepare or review the November 2023 GL 5111 reconciliations in a timely manner. Per our control understanding, Fiscal Analysts are supposed to perform these reconciliations at the end of every month, but the PEBB GL 5111 November 2023 reconciliation wasn't performed until the end of January 2024, and the SEBB GL 5111 November 2023 reconciliation wasn't performed until March 2024. When we inquired with Rita Homan, Deputy Accounting Section Manager, about this, she informed us that HCA tries to perform these reconciliations on a monthly basis, but they weren't able to during this fiscal year due to being short staffed. **See issue linked in conclusion above.**

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **F.6.PR.G - Accounts Payable**

*Procedure Step:* Risk Assessment  
*Prepared By:* EZM, 5/17/2024  
*Reviewed By:* RKM, 9/11/2024

# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

*General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

*Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

## State of Washington

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*



## State of Washington

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation – **HIGH**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

AFRS – Valuation

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## State of Washington

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation – **High**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

**Valuation** - We will use the sampling spreadsheet to determine our sample size. We will test year-end accruals to ensure that the valuation of the accrual is properly supported (invoice amount).

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **F.6.PR.G - Accounts Payable**

*Procedure Step:* Risk Assessment

*Prepared By:* EZM, 5/17/2024

*Reviewed By:* RKM, 9/11/2024

Purpose/Conclusion:

#### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

#### **STEP 1: Inherent Risk (IR)**

## State of Washington

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if

## State of Washington

setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation – **HIGH**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

AFRS – Valuation

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation – **High**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

# State of Washington

**Valuation** - We will use the sampling spreadsheet to determine our sample size. We will test year-end accruals to ensure that the valuation of the accrual is properly supported (invoice amount).

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## G.1.PRG - Due From Other Governments

*Procedure Step:* Summary & Conclusion

*Prepared By:* EJB, 10/4/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **one** modification was deemed necessary to the risk of material misstatement as assessed in planning. See the audit issue detailed in the substantive testing ROWD [[Substantive Test](#)]. See audit issue here [[V: ECY\\_Application of Loan Payments](#)].

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

## State of Washington

*If the results of substantive testing indicate a need to change control risk, auditors should also update the [Permanent File](#) by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

## State of Washington

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of the substantive tests indicated a need to modify our risk assessment. We initially assessed the RMM as low given that there were no prior year valuation issues, and that the automated process for eHub has not been an issue in prior years. The current year issue referenced above resulted in the need to raise the RMM from low to mod, which resulted in the sample size being raised from 21 to 29. The additional samples met all tests without error.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **G.1.PRG - Due From Other Governments**

*Procedure Step:* Understanding of Line Item



# State of Washington

*Prepared By:* EJB, 7/9/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed

## State of Washington

significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

One prior audit exception has been noted in the Department of Ecology - Clean Water State Revolving Fund financial statements surrounding classification issues between short term and long term receivable. However, this will not be an issue for the ACFR as the statement of financial position is not classified.

#### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

#### **Background**

The Clean Water State Revolving Fund (CWSRF), using funding provided by the Environmental Protection Agency (EPA), provides loans to eligible recipients for water infrastructure projects. The funding is made available to local government entities for projects such as updating or

# State of Washington

constructing treatment centers, creating national estuary programs, improving energy efficiency, and reusing/recycling of waste water/storm water among other eligible uses.

The loans receivable balance represents the principal receivable for water infrastructure loans in the upcoming fiscal year plus any accrued interest. Loans receivable is not reduced by an allowance for doubtful accounts. Loan recipients have never defaulted on loans in the history of the program. Loan recipients are incentivized to make timely payments and close their loan so they will be granted low interest or forgivable loans in the future. We determined that it is reasonable for the CWSRF to not maintain an allowance for doubtful accounts.

Accrued interest is recorded from the time of the last payment received in the current fiscal year, to the current fiscal year end.

### **(3) Updates to Significant Account Matrix:**

We noted no updates to the Significant Account Matrix.

### **G.1.PRG - Due From Other Governments**

*Procedure Step:* Controls - eHub  
*Prepared By:* EJB, 7/18/2024  
*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion.:

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy.:

#### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.

In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

Who or what initiates the control

When (or how often) is the control applied

## State of Washington

Who performs the control

As needed, the experience, knowledge and attitude of the person applying the control

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any exceptions or alternative processing to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Financial Statement Audits](#) Planning Guide

Record of Work Done:

#### **Significant Balance(s) and Assertions**

Internal controls in eHub address the following balance(s):

Due From Other Governments

For the following assertion:

Valuation - There is a risk that loans receivable could be miscalculated due to errors in the application of payments or errors in amortization.

#### **1. Gain an Understanding of Internal Controls**

We met with Carla Clarey, Revenues Manager, and Beth Swanson, Senior Financial Advisor, on June 3, 2024 to gain an understanding of controls over loans receivable (controls are consistent with prior year, and there were no changes to the process in FY24).

#### **Loan Creation/Fund Disbursement**

Carla explained that the loan process begins with the agreement between the Department of Ecology and the loan recipient. Agreements are structured using a loan agreement template within Ecology's Administration of Grants and Loans system (EAGL). The language remains similar between agreements but key information such as interest rates, loan lifetime, loan amounts are added to the template agreement. The agreement goes through a system of reviews to ensure accuracy of loan details and sent to the loan recipient for signature.

The loan amount from the signed agreement will be encumbered to allocate funds towards that loan. The loan interest rate and number of years is input from the signed agreement. Per Carla, all information input into the Ecology Helping Unify Business software system (eHub) undergoes a second review by a supervisor. Generally, a Fiscal Analyst 2 will enter information (loan interest rate, loan amount, length of loan from loan agreement) into eHub, a Fiscal Analyst 4 or Clara will review eHub entries for accuracy based on loan agreement details. The actual loan receivable balance is only increased as they get payment request progress reports (PRPRs) to create payments and disburse the funds.

Deferred interest also accrues on a monthly basis from the first payment until the loan is finalized. When the project is completed, the loan amortization schedule is created based on the final loan amount and loan terms. After the amortization schedules have been finalized, they are sent to loan recipients with their final loan agreement, final contract, and the client signs the contract.

## State of Washington

The amortization schedules provide expected values for upcoming principal payments so long as the loan recipient sticks to the repayment plan. If the recipient falls behind (rare) or pays portions or all of the loan off early (common), the remaining principal will not tie to the original amortization schedule. Early payments remove principal owed from the end of the loan (last payment) and does not influence the amount of interest in earlier scheduled repayments. eHub will track and adjust actual/expected payment amounts within the Loan Customer Payments Screen if there were changes to the original payment schedule as a result of early repayment. The loans receivable balance (expected payments) are calculated and created by eHub based on loan agreement information and actual loan transactions **(Key Control 1 - Valuation - Automated Software Calculation)**

### **How Transactions are Recorded in AFRS:**

#### Reclassification

eHub creates a JV that automatically pulls the amounts and puts them into account coding to transfer funds from 1652 (long-term) to 1352 (short-term) for the portion of the loan excepted to be paid in the next fiscal year based on the amortization schedules. eHub creates JVs based on manual entries of key loan information from the system and should match loan agreement details. The coding is prepared in the JV by eHub, staff only need to add the current document number to make the account transfer. Staff performs a manual review of the JVs. There are also smaller adjustments made when a loan goes into repayment throughout the year as loans close out and their amortization schedule is finalized.

At year end, reclassification is done annually based on the amortization schedules. Finance staff attempt to reconcile known adjustments from the amortization schedules through a GL 1352-1652 adjustment worksheet. Due to limitations of eHub system reports, and issues that occurred during system conversion, finance staff has not been able to fully reconcile or determine differences of short term/long term amounts receivable between AFRS and eHub. When the legacy system was converted to eHub, long term balances loaded incorrectly as short term. Per Beth, entries within eHub also may not be accurately recorded as short term/long term due to issues with transaction codes not being recognized by the eHub system. Without any reliable system reports, eHub remains unreconciled to reported balances. This will not be an issue for the ACFR audit as there is not a classified statement of financial position.

Beth performs a reconciliation between eHub's AR subsidiary ledger and AFRS using a Webi query of AFRS GL 1352 and 1652 data to ensure amounts were properly valued **(Key Control 2 - Valuation)**. She uses the 1352-1652 worksheet that uses webi query data and loan status information from eHub to make adjustments. She reviews the 1352-1652 worksheet to identify accounts:

- that have paid their loans off during the year
- signed their agreement late
- have a deferred payment period over the next fiscal year
- amendments to loans
- other changes to loan payment amounts.

Beth will make the appropriate adjustment based on the above and document final amounts to be reported in AFRS.

#### Accrued Interest

## State of Washington

Carla explained that at year-end they run a report from eHub that pulls all accrued interest on loans from their last payment in the fiscal year through June 30. eHub calculates accrued interest by the last payment date recorded in the system for each loan through June 30th and calculates accrued interest due in mid August. This amount is recorded in AFRS via JV to add to the loan receivable balance for this interest earned (**Key Control 3 - Valuation**). A Fiscal Analyst 2 will create the JV, a separate fiscal staff member will review the JV to ensure amounts are reasonable before it is sent to AFRS. The reviewer will typically review the last payment date/accrued interest and compare for reasonableness based on historical interest payments. The year end report also calculates the anticipated payments for the next fiscal year.

### Key Controls are as Follows:

**Key Control 1 (Valuation) - Automated Software Calculation - eHub calculates the loans receivable balance based on the final loan amount, loan terms and actual loan payments tracked by the system.**

**Key Control 2 (Valuation) - Beth Swanson, Senior Financial Advisor, performs a reconciliation between eHub's AR subsidiary ledger and AFRS using a Webi query of AFRS GL 1352 and 1652 data to ensure amounts were properly valued.**

**Key Control 3 (Valuation) - Beth Swanson, Senior Financial Advisor, records deferred interest in AFRS via JV to add to the loan receivable balance for interest earned.**

### Noted Weaknesses are as Follows:

No weaknesses have been noted.

### G.1.PRG - Due From Other Governments

*Procedure Step:* Key Control 1 (Automated)

*Prepared By:* EJB, 8/13/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To determine whether **Key Control 1 (Valuation) - AUTOMATED SOFTWARE CALCULATION - eHub calculates the loans receivable balance based on the final loan amount, loan terms and actual loan payments tracked by the system** - was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.



# State of Washington

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - eHub\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

## State of Washington

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

## State of Washington

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

## State of Washington

What transactions, data, tasks, or documents are approved?  
Who are the preparers? How do preparers submit for approval?  
Who are the authorized approvers? Are there backup approvers?  
What documents or information are required to make approval judgment?  
What is the next step once a transaction/data/ task/document is approved or denied?  
Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

## State of Washington

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each*

## State of Washington

*significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is*

## State of Washington

*controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

## State of Washington

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change*



## State of Washington

*management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in*

## State of Washington

*place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

## State of Washington

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

#### **Automated Interfaces:**

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

## State of Washington

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.

If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

## State of Washington

Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.

If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

# State of Washington

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: "**This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited**".

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

## **Manual vs. Automated Interfaces**

## State of Washington

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered “manual” since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient’s age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient’s name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

# State of Washington

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.



## State of Washington

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.:
-----------------------

### **Due from Other Governments - Valuation**

**Key Control #1 - Automated Software Calculation - eHub calculates the loans receivable balance based on the final loan amount, loan terms and actual loan payments tracked by the system.**

The understanding for this system is documented above in the "Controls - [[Controls - eHub](#)]" step.

### **STEP 1: Understand Automated Key Control**

The loan amount from the signed agreement will be encumbered to allocate funds towards that loan. The loan interest rate and number of years is input from the signed agreement. Per Carla Clarey, Revenues Manager, all information input into the Ecology Helping Unify Business software system (eHub) undergoes a second review by a supervisor. Generally, a Fiscal Analyst 2 will enter information (loan interest rate, loan amount, length of loan from loan agreement) into eHub, a Fiscal Analyst 4 or Clara will review eHub entries for accuracy based on loan agreement details.

## State of Washington

The actual loan receivable balance is only increased as they get payment request progress reports (PRPRs) to create payments and disburse the funds.

Deferred interest also accrues on a monthly basis from the first payment until the loan is finalized. When the project is completed, the loan amortization schedule is created based on the final loan amount and loan terms. After the amortization schedules have been finalized, they are sent to loan recipients with their final loan agreement, final contract, and the client signs the contract.

The amortization schedules provide expected values for upcoming principal payments so long as the loan recipient sticks to the repayment plan. If the recipient falls behind (rare) or pays portions or all of the loan off early (common), the remaining principal will not tie to the original amortization schedule. Early payments remove principal owed from the end of the loan (last payment) and does not influence the amount of interest in earlier scheduled repayments. eHub will track and adjust actual/expected payment amounts within the Loan Customer Payments Screen if there were changes to the original payment schedule as a result of early repayment. The loans receivable balance (expected payments) are calculated and created by eHub based on loan agreement information and actual loan transactions.

### **STEP 2: Confirm and Test Automated Key Control:**

In order to confirm the control, we looked in eHub at Loan ID EL190167 and performed a recalculation of the beginning and ending balance the loan should be at (beginning balance at 7/1/2023 and ending balance at 6/30/2024) and verified that the loan balance at year end was calculated correctly and ties to what is reported. The beginning balance was \$23,967,096.12 (recalculated and tied), the disbursed principal payments were \$1,279,935 (recalculated and tied), the deferred interest payments were \$672,403 (recalculated and tied), and the total payment of \$1,952,338 (recalculated and tied), and the total receivable amount is \$22,014,758.12 at year end (recalculated and tied to year end balance as reported in eHub taken from the amortization schedule). The amortization schedule appears to be properly calculating the year end loan balance as designed. We noted no errors in recalculation or confirmation of the above control.

### **STEP 3: Understand General IT Controls**

The general IT control for due from other governments surrounds loan amortization schedule creation and electronic approval. We met with Beth Swanson, Senior Financial Advisor, and Carla Clarey on 6/13/2024 via MS Teams to discuss and update our understanding of the general IT controls.

**Per Carla, changes can only be made to automated controls by the third part vendor (Azure in this case) and not by anyone at ECY. ECY has no access to edit Azure. In order to request changes be made, Fiscal Analyst 4's may submit a ticket to eHub and then eHub makes the appropriate requested changes in a sandbox (isolated) environment provided by a third party called Azure (General IT Control).** The loan amortization schedule creation is then tested by Carla in this controlled sandbox environment. If Carla deems the change solves the issue submitted on the ticket, she sends approval to eHub to put the change into production.

Carla noted that changes are rarely made to the software. This has only happened twice since 2020 and they were for minor changes to the amortization schedule start date issues. In 2020, some loans that were being created did not reflect the start date input by the loan preparer. Since the ticket was submitted in eHub and the change was tested and approved, this has not been an issue.

## State of Washington

After a loan has been edited or changed in eHub, changes and approvals are done in via email. The loan administrator is the one that approves any changes made - typically Kerry Lines or Lisa Freuderick. There is currently no set policy on how often loan approvals are verified - Carla noted loan amortization schedule approvals are randomly spot checked and each spot check in the current year has shown that loan changes are approved.

### **STEP 4: Confirm Key General IT Controls**

In order to confirm that **changes are made to eHub's calculational inputs only by Azure and no one at ECY**, we examined the spreadsheet that was used in the sandbox testing through Azure. We noted the change on 7/18/2023 that was made was to verify that when an unscheduled payment entered into eHub, the amortization schedule adjusts accordingly. We examined the email showing the requested change (between Amber Aaron, Managed Service Team Lead at HSO - the third party organization that provided the sandbox testing in Azure, and Emily Haeger, (eHub Fiscal Business Analyst), examined the spreadsheet used to show the recalculation produced by eHub (tested in Azure), and noted an email between Emily Hargar, Janis Henry, Financial Systems Business Unit Manager at ECY, and Carla Clarey, Revenue Receivables Manager at ECY confirming the changes made and noted her approval saying she tested the information and noted it looks correct. We noted no errors in confirmation of this control.

### **G.1.PRG - Due From Other Governments**

*Procedure Step:* Key Control 2 (Manual)

*Prepared By:* EJB, 10/2/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm - **Key Control 2 (Valuation) - The Senior Financial Advisor performs a reconciliation between eHub's AR subsidiary ledger and AFRS using a Webi query of AFRS GL 1352 and 1652 data to ensure amounts were properly valued.** - in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls. In testing, however, we noted one instance where the reconciliation process does not appear to be operating as it was designed. See below for more information, and see the audit issue here [[V](#)]:

# State of Washington

ECY Application of Loan Payments].

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important*

## State of Washington

*enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria.7

### **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 2 (Valuation) - Beth Swanson, Senior Financial Advisor, performs a reconciliation between eHub's AR subsidiary ledger and AFRS using a Webi query of AFRS GL 1352 and 1652 data to ensure amounts were properly valued.**

The understanding for this system is documented above in the "Controls - eHub [[Controls - eHub](#)]" step.

## **1. Confirmation of Key Manual Control:**

To ensure amounts are accurately valued, Beth and Carla use the webi query of loans receivable data (1352 and 1652) and identify accounts with activity recorded after year end, amended loans, or deferred payments and make correcting entries and adjustments to loans receivable based on the webi query report and note the changes in the 1352-1652 excel spreadsheet. This includes removing loans that have agreements signed after year end that were included in the financial statement balance and correcting loans with incorrectly posted payments.

We reviewed the reconciliation of eHub's subsidiary ledger as compared to AFRS Webi Query noting the total balance in eHub ties to what is recorded in AFRS for GL accounts 1352 and 1652. On the population spreadsheet used to pick the sample, we noted that the total balance of the loans receivable (due from other governments) ties to what is recorded in AFRS. This population spreadsheet is derived from eHub's AR subsidiary ledger, which was also reviewed and ties to the spreadsheet. ***No issues noted.***

**During substantive testing, we noted the following weakness:** When Beth was preparing the reconciliation, she noted that she mistakenly applied all November payments for each loan to one loan that was part of our testing sample. However, the payments were applied to their respective loans in eHub. We deem this an issue as the reconciliation process is not operating as designed. See issue above in conclusion.

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

## State of Washington

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

#### **G.1.PRG - Due From Other Governments**

*Procedure Step:* Key Control 3 (Manual)

*Prepared By:* EJB, 10/2/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm - **Key Control 3 (Valuation) - The Senior Financial Advisor records deferred interest in AFRS via JV to add to the loan receivable balance for interest earned** - in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

## State of Washington

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*



## State of Washington

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 3 (Valuation) - Beth Swanson, Senior Financial Advisor, records deferred interest in AFRS via JV to add to the loan**

# State of Washington

## receivable balance for interest earned.

The understanding for this system is documented above in the "Controls - [[Controls - eHub](#)]" step.

### **1. Confirmation of Key Manual Control:**

We received the JVs to accrue interest for loans - JV# 46104581 & 46104581-01 on 9/25/2024, confirming that deferred interest was calculated and entered into AFRS and confirmed the interest was added to the loan receivable balance at year end. The JV was traced to support provided for the population used to select the sample. Deferred interest was accrued and added into the total loan receivable balance as of 6/30/2024 as the population support ties to the state balance in AFRS. Interest calculated for Loan ID# EL150024 was \$364.68. This amount was traced to the population document (a list of all loans at 6/30/2024 that ties to AFRS) and we noted no errors. ***No issues noted.***

### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **G.1.PRG - Due From Other Governments**

*Procedure Step:* Risk Assessment

*Prepared By:* EJB, 8/13/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion.*
----------------------

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

#### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

#### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

#### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

#### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

#### *Inherent Risk due to Non-Compliance*

## State of Washington

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?  
Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?  
Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

## State of Washington

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation - Moderate

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

eHub - Valuation

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant

# State of Washington

class of transactions:

Valuation – Moderate

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

We plan to use the Ecology Helping Unify Business software system (eHub) to perform testing of the loans receivable balance. We will search for the selected loan ID number on the Loan Management > Loans > All loans screen to determine if recorded loans receivable amounts were accurately valued. Then we will use the loan transactions screen and the amortization schedule to recalculate loans receivable based on actual payments.

Verify that eHub receivables have reconciled to AFRS.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## **G.1.PRГ - Due From Other Governments**

*Procedure Step:* Substantive Test

*Prepared By:* EJB, 10/22/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion.\*

### **Purpose:**

To determine whether receivables were reported at properly valued or calculated amounts (Valuation).

### **Conclusion:**

We determined receivables were properly valued, however the reconciliation process does not appear to be operating as it was designed. See below for more information, and see the audit issue here [[V: ECY Application of Loan Payments](#)].

Testing Strategy.\*

# State of Washington

**Add the testing strategy for each relevant assertion from the TeamStore.**

Guidance/Criteria:

**Add the Guidance/Criteria for each relevant assertion from the TeamStore. You may also include other resources that you used for testing.**

Record of Work Done:

**Substantive tests performed to meet the Valuation assertion:**

We used the Ecology Helping Unify Business software system (eHub) to perform testing of the loans receivable balance. We searched for the selected loan ID number on the Loan Management > Loans > All loans screen to determine if recorded loans receivable amounts were accurately valued. Then, we used the loan transactions screen and the amortization schedule to recalculate loans receivable based on actual payments.

On the summary tab of the testing workpaper referenced below, we verified that the eHub receivables reconciled to AFRS without error.

See testing here [[EL190167 Loan Transactions Summary](#)].

**Substantive tests performed to meet the Valuation assertion:**

All testing was performed using eHub to confirm loans were calculated correctly.

we searched for the loan ID# on the Loan Management > Loans > All loans screen to determine if recorded loans receivable amounts were accurately valued.

We used the same loan transactions screens and the amortization schedule to recalculate loans receivable based on actual payments made.

During the testing performed on the worksheet, we determined that one of the loans was not calculated correctly on the PBC 1352-1652 report (the reconciliation to AFRS). Per discussion with Beth, this loan is one of three loans to a specific entity. On the 1352-1652 report, there were payments in November on all three loans. When Beth was preparing the reconciliation, she noted that she mistakenly applied all November payments for each loan to the one loan we selected. However, the payments were applied to their respective loans in eHub. Based on this information, we noted that the process of preparing the reconciliation is a bigger risk than we had initially assessed. We raised the risk of material misstatement to moderate and increased the sample size from 21 to 29. The additional samples met testing expectations without error. We noted that the issue will *not* be projected out as the entire loan balance would not have been understated. However, we still deem this an issue as the reconciliation process is not operating as designed. See issue above in conclusion.

**G.2.PRg - Other Taxes**

# State of Washington

*Procedure Step:* Summary & Conclusion

*Prepared By:* BFW, 11/21/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion.

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy.

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:



# State of Washington

## Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria.:

## **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done.:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

**(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

**(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

## G.2.PRG - Other Taxes

*Procedure Step:* Understanding of Line Item

*Prepared By:* BFW, 6/4/2024

*Reviewed By:* RKM, 6/10/2024

Purpose/Conclusion.:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy.:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

# State of Washington

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

## **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

## **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is*

## State of Washington

*understatement a small or omitted account may hold the most potential for the largest misstatement).*  
*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*  
*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions:**

There were no prior audit exceptions for this line item.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

Other Taxes is made up of the following taxes:

Source 112 - Hazardous Substance Tax (99.98%)

Source 160 - Commercial Fishing - Privilege Tax (0.02%)

Hazardous Substance Tax makes up the majority of the balance, therefore we will focus our control understanding and testing on this source.

Hazardous substance tax is a tax on the first possession of hazardous substances in Washington. The tax applies to petroleum products, certain pesticides, and certain chemicals. Hazardous Substance Tax revenues are determined using the Automated Tax and Licensing Administration System (ATLAS), based on tax returns submitted in the system. ATLAS automatically calculates the Hazardous Substance Tax due based on information provided on the tax return. DOR Tax Examiners verify the documents provided by tax payers to support the amount of taxes due. Tax payments automatically update in the system, which sends the information to AFRS in a nightly batch process. The batch information is reviewed and reconciled by staff in the Business & Financial Services (B&FS) division. Hazardous Substance Tax revenue is accrued in AFRS in the same manner as other taxes receivable are recorded in ATLAS.

### **(3) Updates to Significant Account Matrix:**

We identified no changes that need to be made to the Significant Account Matrix.

## **G.2.PRГ - Other Taxes**

# State of Washington

*Procedure Step:* Controls - ATLAS  
*Prepared By:* BFW, 6/11/2024  
*Reviewed By:* RKM, 10/17/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.
- An expanded description of key controls.

## State of Washington

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

# State of Washington

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls in the Automated Tax and Licensing Administration System (ATLAS) address the following balance(s):

Other Taxes - Hazardous Substance Tax

For the following assertions:

**Occurrence** - There is a risk that recorded revenue is more than source records.

**Valuation** - There is a risk that tax revenues are not recorded at properly valued amounts.

# State of Washington

## **Gain an Understanding of Internal Controls**

We met with Brittany Padilla, Tax Administration Manager - Hazardous Substance, and Liz Black, Program Coordinator, via Teams on April 22, 2024 to gain an understanding of controls.

## **Tax Returns**

The majority of tax returns are received electronically and filed through the online taxpayer system, My DOR, which is part of the State's Secure Access Washington (SAW) application created by the Washington Technology Solutions (WaTech). Returns filed in My DOR are sent directly into ATLAS, which is coded to automatically calculate taxes due based on the information entered by the taxpayer on the return. Taxpayers are typically filing either monthly or quarterly on a combined excise tax return. All businesses conducting in Washington state dealing with the substances outlined in [RCW 82.21](#), petroleum products, certain pesticides, and certain chemicals are subject to hazardous substance tax.

When a taxpayer logs into their My DOR account and selects to file a return, ATLAS automatically calculates taxes due from pre-programmed rates based on return information entered by the taxpayer (**Key Control #1- Automated- Valuation**). When the taxpayer submits the return, taxes due and the payment amount are recorded in the transactions tab of ATLAS. Additionally, information such as the date filed, the date paid, and any changes or adjustments made to the return or the taxpayer's account will also be recorded in the transactions tab of ATLAS. My DOR and ATLAS only allow a return to be filed once and ATLAS will create a work item for duplicate return received if the taxpayer attempts to submit a paper return for the same return period received. Logic checks are run when the return is processed. If there is an error, the return is flagged and sent to a work queue for an Examiner to review. Returns flagged for review do not get recorded to the appropriate revenue source until errors are resolved and released from the queue.

For July 1, 2023 - June 30, 2024 the published rates are \$1.40 per barrel. [WAC 458-20-252](#) explains that under chapter 82.21, a hazardous substance tax is imposed upon the wholesale value of certain substances and products, with specific credits and exemptions provided. Exemptions and deductions claimed for this tax are tracked on a spreadsheet that lists lifelong taxpayers that have taken them. An Excise Tax Examiner (ETE) 3 will review the spreadsheet and reconcile quarterly to ensure taxpayers who are claiming the exemptions or deductions have claimed them previously or verify qualifications for taxpayers who are claiming for the first time (**Key Control #2 - Manual - Occurrence**).

There are two deductions possible: Agricultural Crop Protection Products Exemption RCW 82.21.040 (5), and Other Deductions RCW 82.21.040 (1-4). Taxpayers may be able to take an exemption from the Hazardous Substance Tax if they have possession of agricultural crop protection products that are warehoused, but not used or sold, in Washington. (Engrossed Substitute Senate Bill (ESSB) 6057 Part XIX; Chapter 6, Laws of 2015). This exemption was effective 9/1/2015. Reporting is reviewed quarterly, and each taxpayer is contacted by the ETE3 assigned to the program. An Annual Tax Performance Report (ATPR) is required for this exemption. Anyone reporting the Agricultural Crop Protection deduction is required to submit an annual tax performance report (ATPR). Taxpayers have to file the ATPR timely, and if they do not file this timely then they are billed back for the exemption / deduction that they took. The ETE reviews everything in its entirety. If the spreadsheet reconciliation has not been performed at the time of the ATPR due date, then the ATPR holistic account review would identify any deductions taken that are



## State of Washington

unallowable. In FY23, the total amount of exemptions taken roughly \$19.3 million, or 7% of the balance for Hazardous Substance Tax. This is expected to be similar in FY24.

### **How Transactions are Recorded in AFRS:**

#### **Gross Receipts Accrual Entry**

For monthly filers, excise tax returns for June activity are due July 25th and for quarterly filers, tax returns for the 4th fiscal quarter (April, May, and June) are due July 31st. In August, the ATLAS "gross receipts" report, which is programmed to pull all gross receipts for the period July 1 - August 15, is downloaded to Excel and compared to the gross receipts from the prior five years to check that the values seem reasonable. Revenue Accounting will prepare a JV to enter into AFRS to show the June returns received after June 30<sup>th</sup> as a receivable and accrued revenue for the FYE.

We met with Jerry Tilson, Revenue Accounting Manager, on April 10, 2024 to discuss the gross receipts accrual entry. Jerry explained that towards the end of August, he runs the "gross receipts" report from ATLAS for receipts received between July 1 - August 15 for the tax filing period of June 30 and exports the data to Excel. Once the data is exported into Excel, he sorts by fund and revenue source. The data is then automatically pulled into the "taxpayer assessed taxes (tat) worksheet" tab where the gross receipts are summarized by tax type. Jerry then reviews the report for any errors or major changes and compares the amounts to the prior 5 years for reasonableness. Any significant changes are noted and documented at the bottom of the taxpayer assessed taxes report. After reviewing the report, Jerry verifies that the total gross receipts amount on the "taxpayer assessed taxes report" tab matches the total on the "combined gross receipts adj" tab to ensure that the data from the gross receipts report was pulled in correctly. The JV is then created by pulling the data from the "taxpayer assessed taxes report" tab and input into AFRS by a Revenue Accounting Fiscal Analyst and reviewed and released by Jerry. Additionally, Binh Vu, Accounting Manager, reviews all fiscal-year end JVs. A fiscal analyst reviews the AFRS daily transaction report the next business day to ensure that the accruals were recorded in AFRS accurately and occurred in the correct period.

#### **Cash Journal Entries**

When payments are received via ACH/debit, ACH/credit, wire transfer, and cash/check from field offices, ATLAS automatically generates an A8 cash journal (CJ) to record the cash receipts. For payments received by credit card, lockbox and via mail/FedEx/UPS, a manual CJ is created in ATLAS by Treasury Management in Business & Financial Services (B&FS). Treasury Management staff batch the documents and prepare the deposits assuring they both balance. Once they are entered, the Batch Control System (BCS) compares the total of the individual batches to what was deposited for the day. The A8s are sent to the State Treasurer's Office (OST) for deposit entry into the Treasury Management System and verification that all funds have been received. If the payment amount received by the OST does not match DOR's A8, they will contact DOR and inform them of the out of balance condition. Treasury Management will follow up on the difference by totaling and comparing the documents and payments. The Batch Sheet which contains the batch amount totals, document count, batch date, and batch number is placed on top, and the batch is forwarded to Taxpayer Account Administration (TAA). Treasury Management then reconciles the ATLAS cash journal report totals to the total deposit recorded in the OST's concentration account to ensure they match.

## State of Washington

DOR's Revenue Accounting section in B&FS verifies the CJ batches are error free and releases for processing in AFRS at the end of each day. ATLAS initially records the deposit in Fund 01P (Suspense Account) and then distributes from suspense to the proper revenue source codes once the returns and payments are applied to the taxpayers' accounts. If the payment is identified as Excise Tax but not applied to a tax return, the fund is transferred to the general fund Revenue Act revenue source (01-99 – Tax Revenue Suspense). If tax payments are not applied to the taxpayer's account due to mismatched returns or errors that need to be resolved, the funds will remain in the suspense account until issues are resolved by Tax Examiners. Once the payment has been applied to the taxpayer's account, ATLAS will automatically create a journal voucher to move the funds to the appropriate revenue sources. Batches are created and transmitted to AFRS in the evening. Revenue Accounting reviews the batch the following day and releases them in AFRS.

### **Reconciliation Process**

ATLAS receives a daily reconciliation file from AFRS and performs an automatic reconciliation between the data recorded in AFRS and ATLAS to ensure revenues recorded are accurate and complete (**Key Control #3 -Automated- Valuation/Occurrence**). OFM sends an AFRS download into a SFT folder daily that is picked up by ATLAS. ATLAS then automatically performs a reconciliation between the journal voucher batches in ATLAS from the prior day to the revenues recorded in AFRS. Once the reconciliation is complete, ATLAS will update the batch with the reconciliation date under the "reconciled" column. There have been a few issues where the AFRS file was not received and some batches did not go through the automatic reconciliation. Revenue Accounting reviews each batch in ATLAS for a "reconciliation date" to ensure the reconciliation took place. If the AFRS file is not received, Revenue Accounting will contact OFM for the file. However, if the request is made 10 days or more after the date the batches were processed in AFRS, the AFRS data is no longer available for transmission. If the batch does not go through the automatic reconciliation, Revenue Accounting will perform a manual reconciliation.

### **Key Controls are as Follows:**

**Key Control #1 - (Automated) - Valuation** - When a taxpayer logs into their My DOR account and selects to file a return, ATLAS automatically calculates taxes due from pre-programmed rates based on return information entered by the taxpayer.

**Key Control #2 - (Manual) - Occurrence** - Exemptions and deductions claimed for this tax are tracked on a spreadsheet that lists lifelong taxpayers that have taken them. An Excise Tax Examiner 3 will review the spreadsheet and reconcile quarterly to ensure taxpayers who are claiming the exemptions or deductions have claimed them previously or verify qualifications for taxpayers who are claiming for the first time.

**Key Control #3 - (Automated) - Valuation/Occurrence** - ATLAS receives a daily reconciliation file from AFRS and performs an automatic reconciliation between the data recorded in AFRS and ATLAS to ensure revenues recorded are accurate and complete.

### **Noted Weaknesses are as Follows:**

None.

# State of Washington

## G.2.PR.G - Other Taxes

*Procedure Step:* Key Control #1 (Automated)

*Prepared By:* BFW, 10/16/2024

*Reviewed By:* RKM, 10/17/2024

### Purpose/Conclusion:

#### **Purpose:**

To determine whether when a taxpayer logs into their My DOR account and selects to file a return, ATLAS automatically calculates taxes due from pre-programmed rates based on return information entered by the taxpayer (**key control 1 for ATLAS**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [[Risk Assessment](#)].

### Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

#### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

## State of Washington

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### Automated Interfaces:

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

# State of Washington

## Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

## Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and*

## State of Washington

*follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for*

# State of Washington

*overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **Automated Interfaces:**

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

# State of Washington

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

## Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

## Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

## Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.



## State of Washington

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or*

## State of Washington

*per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the*

## State of Washington

*interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

## State of Washington

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

## State of Washington

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?  
How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

## State of Washington

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Automated Interfaces:

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Computer Generated Reports:

## State of Washington

If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.

If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.

If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance workpaper in the Store.

# State of Washington

## **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:
--------------------

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Information Technology](#) Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This



## State of Washington

process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

## State of Washington

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

## State of Washington

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An "**electronic signature**" can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A "**digital signature**" is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the**

# State of Washington

**Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

**Key Control #4 - (Automated) - Valuation** - When a taxpayer logs into their My DOR account and selects to file a return, ATLAS automatically calculates taxes due from pre-programmed rates based on return information entered by the taxpayer.

## **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

## **STEP 2: Confirm and Test Automated Key Control:**

To confirm the automated control, we re-performed the tax calculations for a sample of tax returns at [\[HST Testing\]](#). See "IT Control Testing - Valuation" tab.

## **STEP 3: Understand General IT Controls**

We gained an understanding of general controls in the Tax Collections for Other Governments section, as the processes are identical regardless of the type of tax being calculated, see here: [\[Key Control 2 \(Automated\)\]](#).

## **STEP 4: Confirm Key General IT Controls**

We confirmed general IT controls in the Tax Collections for Other Governments section, as the processes are identical regardless of the type of tax being calculated, see here: [\[Key Control 2 \(Automated\)\]](#).

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **G.2.PRG - Other Taxes**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* BFW, 6/24/2024

*Reviewed By:* RKM, 10/15/2024

## State of Washington

Purpose/Conclusion.\*

**Purpose:**

To confirm quarterly review of deductions and exemptions for the hazardous substance tax **(Key Control 2 for ATLAS)** in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy.\*

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

## State of Washington

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. *Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. *Controls are not related to a "significant risk" identified in the audit plan.*
- C. *Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all*

## State of Washington

*control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #2 - (Manual) - Occurrence** - Exemptions and deductions claimed for this tax are tracked on a spreadsheet that lists lifelong taxpayers that have taken them. An Excise Tax Examiner 3 will review the spreadsheet and reconcile quarterly to ensure taxpayers who are claiming the exemptions or deductions have claimed them previously or verify qualifications for taxpayers who are claiming for the first time.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

We obtained the spreadsheet reconciliation for Q1 of FY24. We noted one tab of the document was for crop protection deduction. There were 4 taxpayers listed, three of which had three months worth of filing periods noted and one had two months worth of filing periods, all listed as verified with the dates they were initially verified as qualifying for this deduction. The reviewer was noted as "HH - 3/24". We noted a second tab for Other Deductions that contained 4 taxpayers, one for three months, two for two months and one for a single month. We noted three of the four taxpayers were verified and date of verification was noted for each. One was noted as not verified, "Request for information - No description given." The reviewer for all but one of these was noted as "HH - 3/24" and the reviewer for the last one was noted as "BP - 4/24". ***No issues noted.***

### **Noted Weaknesses are as follows:**

None.

# State of Washington

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **G.2.PRG - Other Taxes**

*Procedure Step:* Key Control #3 (Automated)

*Prepared By:* BFW, 6/20/2024

*Reviewed By:* RKM, 10/17/2024

Purpose/Conclusion:

### **Purpose:**

To determine whether daily reconciliation between ATLAS and AFRS (**key control 3 for ATLAS**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [Risk Assessment].

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:



# State of Washington

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

## State of Washington

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and*

# State of Washington

*transaction processing controls.*

## Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

## Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

## State of Washington

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

# State of Washington

## Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

## Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

# State of Washington

## Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

## Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

## Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

## State of Washington

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables*

## State of Washington

*or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*



## State of Washington

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

## State of Washington

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3

## State of Washington

is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### Software Calculation:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Automated Interfaces:

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

## State of Washington

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Information Technology](#) Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

#### Manual vs. Automated Interfaces

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the*

# State of Washington

*following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process

## State of Washington

to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm



# State of Washington

with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**Key Control #3 - (Automated) - Valuation/Occurrence** - ATLAS receives a daily reconciliation file from AFRS and performs an automatic reconciliation between the data recorded in AFRS and ATLAS to ensure revenues recorded are accurate and complete.

### **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **STEP 2: Confirm and Test Automated Key Control:**

We met with Ayano Faasumalie, Revenue and Finance Reporting Coordinator, on April 16, 2024 via teams, to walkthrough the daily reconciliation between ATLAS and AFRS. We reviewed a taxpayer account as part of our control 2 confirmation in Retail Sales and Use & B&O that was posted to ATLAS in JV #140E1015 with a batch total of \$312,543,343.99. We reviewed the JV within ATLAS and noted the reconciled column showed JV #140E1015 was reconciled by ATLAS to AFRS 3/28/2024. We then tied out this JV's total to the batch log, created by Revenue Accounting using AFRS data, without exception. *No issues noted.*

### **STEP 3: Understand General IT Controls**

We gained an understanding of general controls over the interface process as part of Taxes Receivable (Net of Allowance) key control 2, which can be seen here: [[Key Control #2 \(Automated\)](#)].

### **STEP 4: Confirm Key General IT Controls**

We confirmed general IT controls as part of Taxes Receivable (Net of Allowance) key control 2, which can be seen here: [[Key Control #2 \(Automated\)](#)].

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed

# State of Washington

at MAX.

## G.2.PRG - Other Taxes

*Procedure Step:* Risk Assessment  
*Prepared By:* BFW, 6/20/2024  
*Reviewed By:* RKM, 10/17/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

#### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

*Inherent Risk due to Error*

## State of Washington

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

# State of Washington

## **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

## **(1) Inherent Risk (IR):**

## State of Washington

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

**Occurrence - Moderate**

**Valuation - Moderate**

**(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**Automated Tax and Licensing Administration System (ATLAS) - MAX - Occurrence, Valuation**

We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

**(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**Occurrence - Moderate**

**Valuation - Moderate**

**(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

**Occurrence** - We will select a sample of registered taxpayers, review ATLAS for a filed return, and tie return to AFRS to ensure revenue occurred in the current year and is complete.

**Valuation** - We will recalculate taxes paid for the same sample noted above of registered taxpayers to ensure taxes are recorded at proper values

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

**G.2.PRГ - Other Taxes**

*Procedure Step:* Substantive Test

*Prepared By:* BFW, 10/15/2024

# State of Washington

*Reviewed By:* RKM, 10/17/2024

Purpose/Conclusion:

**Purpose:**

To determine whether reported revenues represent actual amounts relating to the period.  
To determine whether revenues were reported at properly valued or calculated amounts.

**Conclusion:**

We determined reported revenues represent actual amounts relating to the period and revenues were reported at properly valued or calculated amounts. *No issues noted.*

Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

**Cut-Off / Revenue Recognition**

Test transactions recorded in the current period to verify the revenue occurred during the period.

*Transactions recorded at the beginning and end of the current period would generally be considered at highest risk of being improperly recorded in the current period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields.*

# State of Washington

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

## **Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

## **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the completeness assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Identify expected revenue streams based on understanding of fund activities and scan to see if revenue is reported for all such streams.

Follow up on any unexpectedly missing streams.

Identify new revenues (ex: new grants or programs) and follow up to verify that expected revenues have been reported.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Trace selected or sampled revenues from source documents to accounting records.

*Source documents may consist of billing, fine, or fee records. Or it may consist of service records that imply a billing, such as license or permit issuance.*

Perform a multi-year trend of revenues and follow up on unexpected decreases.

Search for manual journal entries that debit (decrease) revenues. Consider testing if any risk indicators are noted.

# State of Washington

## Cut-Off

Test transactions recorded in the next period to determine whether the revenue should have been recorded in the current period.

*Transactions recorded at the beginning of the next period would generally be considered at highest risk of being improperly shifted to that future period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields. If the population is large, consider stratifying to either scan and select or test 100% of all large value transactions combined with a lower assurance sample for small dollar transactions.*

## Detail Roll-up

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## Calculation

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

## Realizable Value

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

## Estimation / Recognition

Review calculation and support for assumptions of any estimated revenues.



# State of Washington

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

Guidance/Criteria:

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS 3.6.13 Utility Tax (*applies only to cities*)** - should be accounted for as a revenue in the general fund (3164000) and expenditure in the utility fund (53P0040), if the utility passes the tax on to its customers then the additional charges should be recognized as revenue (343P000) directly in the utility fund not in the general fund

## **BARS 3.6.11 Suspense Funds**

Record of Work Done:

### **Population**

To ensure testing provided a sufficient amount of coverage of the Hazardous Substance Tax balance, we obtained our population and broke out the taxes by fund and sources to ensure amounts we tested represented the whole balance. We obtained a query from ATLAS from Ayano Faasualie, Revenue & Financial Reporting Coordinator, that included all payments made by taxpayers that included hazardous substance tax. We tied the totals directly to the monthly revenue activity (MRA) spreadsheet prepared by Revenue Accounting at DOR and provided by Jerry Tilson, Revenue Accounting Supervisor. We used the MRA spreadsheet to break out each tax type by fund and source and tied amounts to the ACFR line item lead sheet [[Line Item Lead Sheet](#)]. See our reconciliation as part of testing at [[HST Testing](#)], in tab 'Testing Summary.' Amounts tied without exception. We considered the population complete and provided coverage over the whole ACFR balance. ***No issues noted.***

Using the revenue query ran from ATLAS noted above, we haphazardly selected a sample of 30 transactions (payments made to a taxpayer account for a single filing period) and used the same sample to ensure amounts reported in AFRS occurred in the current year and accurately valued. See more details for each assertion below.

### **Substantive tests performed to meet the Occurrence assertion:**

To ensure reported revenues represent actual amounts relating to the period, we performed the following substantive tests:

- FY24 return was filed for taxpayer
- Ensured tax revenue was recorded to batch processed in ATLAS for the correct period
- Ensured batch total processed in ATLAS ties to batch total recorded in AFRS

For each selection, we reviewed screen shots of the revenue tab within the taxpayer's account and history sub tab to identify the tax return for

## State of Washington

the correct filing period, provided by Ayano Fassuamalie, Revenue & Financial Reporting Coordinator. Within ATLAS, there was a hyper link for the ATLAS receivable accumulation that the transaction was included in and could be followed from there and we were provided screen shots of this. We traced each taxpayer account to the ATLAS accumulation and matched the batch total in ATLAS to the year end entry to AFRS using additional screen shots of these items. Based on the tax type, we ensured the revenue was included in the correct balance. ***No issues noted.*** See testing performed at [\[HST Testing\]](#).

### **Substantive tests performed to meet the Valuation assertion:**

To determine whether tax revenues were reported at properly valued or calculated amounts, we performed the following substantive tests:

Recalculated retail sales, use, and B&O taxes for the selected taxpayer

During review of controls, we noted ATLAS automatically applies tax rates for hazardous substance taxes and automatically calculates taxes due. To test the IT control, we re-performed calculations for a sample of 30 taxpayers as documented at [\[HST Testing\]](#) in the "IT Control Testing - Valuation." We noted that all taxes recalculated tied to the taxes owed and paid in ATLAS and determined that revenues were reported at properly valued and calculated amounts. ***No issues noted.***

### **G.3.PRG - Licenses, Permits and Fees**

*Procedure Step:* Summary & Conclusion

*Prepared By:* EJB, 9/9/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion.:

#### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

#### **Conclusion:**

We determined that no modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy.:

# State of Washington

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?

## State of Washington

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

#### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

#### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

# State of Washington

## G.3.PRГ - Licenses, Permits and Fees

*Procedure Step:* Understanding of Line Item

*Prepared By:* EJB, 7/16/2024

*Reviewed By:* RKM, 12/17/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and

## State of Washington

which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

In the prior year ACFR, there was a classification issue. The Dept. of Ecology (ECY) included the revenue from the CCA (Climate Commitment Act) Auction in Misc. Revenue. We noted that this should be grouped with license, permits and fees.

We emailed Kennesy Cavanah (statewide accountant) at OFM. She noted that this has been corrected in the current year, and confirmed the sort code has been changed to CD - Licenses, Permits, and Fees.

# State of Washington

## **(2) Composition & Change Analysis:**

Line Item Lead sheet: [\[Line Item Lead Sheet\]](#).

The CCA Auction revenue was introduced in FY23. It is reported as a "License Permit and Fee" and is treated as an exchange transaction. This is because ECY is selling the right to participate and trade the allowance in the open market and not right to use the allowances. When auction participants wish to sell allowances, they would then transfer them back to ECY to be included in the next auction. The proceeds from the sale are transferred to the appropriate auction participant. Based on our understanding of sale of allowances as an exchange transaction, we consider that revenue is earned when allowances are sold. The allowance do not meet the definition of assets or liabilities based on a technical inquiry with GASB. Per GASB Concept Statement number 4, "Assets are resources with present service capacity that the government presently controls." This revenue represents the sales of "allowances" to various entities that produce emissions. The allowances provide these entities the ability to produce emissions, with allowances sold decreasing year over year in an attempt to reduce emission production in Washington.

Cap-and-Invest Auctions are held four times per year, once per quarter. The participants register through a software called Compliance Instrument Tracking System Service (CITSS) which is where they bid on allowances and trade the allowances as desired by approved participants. At each auction, a set number of allowances (announced prior to the auction) go up for auction. These auctions are sealed-bid auctions, meaning that participants submit a bid that is not seen by anyone except the Climate Commitment Act Implementation Group (CCA IG) that distributes the allowances. Participants can submit a single bid for all desired allowances or a series of bids for various groups of allowances. Bids are sorted, highest to lowest, and allowances are allocated to each bid in that order. Once all allowances listed for auction have been assigned to a bid, the lowest \$ bid that won an allowance is the price that *all* participants pay. Participants that did not win an allowance will have to bargain for them on the CITSS Market, where winning participants may choose to sell their allowances (not dissimilar to a stock market).

There can be additional auctions throughout the year that are triggered when one of the quarterly auctions' settlement price is higher than a pre-determined number. These auctions are called Allowance Price Containment Reserve Auctions (APCR). There were two APCR Auctions in the current year as the settlement price for the June 2023 Auction (\$56.01) was in excess of the 2023 pre-determined settlement price trigger (\$48.30 for FY23), and the settlement price for the August 2023 Auction (\$63.03) was in excess of the 2024 pre-determined settlement price trigger (\$51.90 for FY24).

No-cost allowances are allowances issued to "clean" energy utilities. These utilities may "consign" these allowances to be sold in auction. This means that the utility company transfers the no-cost allowances back to the Dept. of Ecology to sell at auction on behalf of the utility company. These funds should never be recorded as revenue for the Dept. of Ecology. We would expect to see a list of these allowances sold and would expect to see them separate from revenue.

The GL account is 3210 and the fund codes are 26A & 26B. The majority of this line item is the aforementioned CCA Auction revenue. The remainder of this line item is insignificant to the Wildlife and Natural Resources Opinion Unit.

# State of Washington

## **Line item Summary:**

CCA Auction revenue is the only material revenue recorded in this account.

## **(3) Updates to Significant Account Matrix:**

There are no changes to the significant account matrix from what we have learned above.

## **G.3.PR.G - Licenses, Permits and Fees**

*Procedure Step:* Controls - Auction Platform

*Prepared By:* EJB, 7/18/2024

*Reviewed By:* RKM, 12/17/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.



## State of Washington

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented. Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

## State of Washington

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls in the Auction Platform address the following balance(s):

# State of Washington

License, Permits and Fees

For the following assertions:

Valuation - There is a risk Ecology has not calculated auction revenue proceeds correctly for this new program.

Completeness - The final auction for the fiscal year will likely require the posting of a receivable and there is a risk this revenue will not be reported in the correct fiscal year.

## **Gain an Understanding of Internal Controls**

We set up a MS Teams call with Beth Swanson, Senior Financial Advisor, Derek Nixon, Cap-and-Invest Section Manager, and Carla Clarey, Revenues Manager, at the Department of Ecology on June 3, 2024. We went over internal controls and internal processes in place regarding the Climate Commitment Act (CCA) Auction Revenue. We also noted that the software used by ECY for recording revenue transactions and year end receivables is eHub. eHub has been used by ECY for many years, and Beth and Carla are both familiar with how to use this software. Below is the process of deposit distribution, along with internal controls included:

## **Climate Commitment Act Auction Process:**

Deutsche Bank (DB) serves as the Financial Services Administrator (FSA) for the Cap-and-Invest Program's allowance auctions. After the auction has been scheduled, the ECY will release the amount of allowances to be sold at the auction (decided through legislation). Auctions are sealed bid auctions and the participants submit their bids through the auction platform software controlled and ran by the Western Climate Initiative (WCI). When bids are received, the auction platform sorts bids by highest to lowest, assigning allowances top to bottom until all allowances have been assigned. Below is the time line for the entire process, along with hypothetical dates to provide an illustration:

Auction Occurs - 2/28.

CCA IG determines settlement price and transmits to DB - 3/7 (5 business days).

CCA IG publishes Auction Summary Results Report on web site - 3/7 (5 business days).

DB obtains payments from winning bidders and collects funds by this date - 3/15 (11 business days).

DB notifies CCA IG when/whether payments are received and processed from qualified bidders by this date - 3/15 (11 business days).

CCA IG provides Fiscal Office amounts for each account 3/27 (27 calendar days).

DB transfers state-owned proceeds to US Bank and US Bank notifies OST - 3/28 (28 calendar days) - the remainder of the below steps all occur on 3/28, or 28 calendar days later).

OST creates ACH Accounts Receivable Report and the Wire Accounts receivable Report.

Fiscal Office downloads reports and records payment information.

Fiscal transfers A-8 cash journal to OST.

OST deposits revenue as instructed by ECY.

CCA IG publishes Washington Auction Public Proceeds Report on web site.

## State of Washington

Compliance Instrument Tracking System Service (CITSS) calculates who is eligible to participate in the auction based on inputs established by WCI and legislation. The Auction Platform (WCI) sets purchase limits, holding limits, and bid guarantees based on the structure of the upcoming auction. This information is released when the auction is announced. The holding limits are based on emission needs and the bid guarantees are based on a combination of holding limits and the participant's desired allowance purchases. The floor price for the auction is set by the ECY. When an auction participant bids, the only time a bid is rejected is if the bid is below the floor price. Each bid has a unique ID so that the Auction Platform, ECY, and the market participant can easily identify each transaction made. WCI hosts the auction platform and is contracted to provide third party analytics for these auctions which end up being the driving force for the revenue amounts recorded. Bidders are notified if they are qualified two days before the auction takes place. They have 12 days before auction to submit the bid guarantee. Qualified bidders are available online to the public at all times via a public records report. All submitted bids for all entities are reported in the bids report. ECY monitors the bid reports in real time during auctions. This helps catch and possible issues. The lowest bid that won an allowance now becomes the price that each participant pays for their respective awarded allowances. The CCA IG is an internal group created by the ECY. This team is made up of Derek Nixon, Cap-and-Invest Section Manager (leader of the CCA IG), Mike Johnson, Cap and Invest Auction Lead, Scott Hancock, Senior Market Monitor, and a few other people on the ECY CCA team. The CCA IG was formed to assist with the establishment of processes surrounding the CCA revenue. This team helps calculate and verify amounts are correct and are ready to be recorded as revenue. Upon completion of the auction, WCI sends the bid information to ECY. The auction platform (ran by WCI) calculates all bid and results reports that drive the calculation of funds to be received from DB and then recorded by the ECY (**Key Control #1 - Valuation - Automated**) CCA IG. Scott Hancock (Senior Market Monitor) developed a source code that he runs (via RStudio) to confirm the bid holding limits, the qualified bidders report, the bid guarantees, and the bid assignments (for bids that won an allowance and bids that did not win an allowance). Scott uses this source code to recalculate and verify that all information produced by the auction platform is accurate and calculates correctly. The information is then transmitted to DB.

The CCA IG publishes the Auction Summary Report on Ecology's Auctions and Trading web page here: [Climate Commitment Act Notices and Reports](#). The report will be similar in format and content to the California Air Resource Board's (CARB) [Summary Results Report \(ca.gov\)](#).

### **Collection and Transfer of Auction Funds:**

DB obtains payment from winning bidders, reconciles accounts, and collects funds. Bidders must submit cash, bond, or letter of credit at least 12 days in advance of the auction day and DB holds these funds (the bid guarantee) in escrow. Auction winners are notified via a financial statement and a financial settlement report. These reports are sent to each winner as an "invoice" that details the amount of allowances won, the amount paid per allowance, and the total cost and amount that will be transferred to DB. For each winning bidder, funds are taken from that bid guarantee and the remaining balance, if any, is returned to the bidder 26 days after auction.

DB notifies the CCA IG when/whether payments are received and processed from qualified bidders. The CCA IG then determines which funds are from consigned no cost allowances and which funds are from sold allowances that may be recorded as revenue. This process is simple as the amount of consigned allowances in each auction is determined before the auction occurs. The revenue from

## State of Washington

these allowances are simply the bid settlement price times the amount of consigned allowances. Consigned allowances are allocated annually to each eligible electrical distribution utility or natural gas supplier (consigning entity). A consigning entity consigns these allowances to be sold in the quarterly auctions over the course of the year. For 2023, allowances will be transferred mid-year after the CCA IG has finalized allocation calculations. This won't occur until the second, third or fourth auction. All proceeds from the auction of consigned allowances will be used for the benefit of ratepayers, which, for investor-owned utilities, will be determined by the Utilities and Transportation Commission (UTC). The auction platform (WCI) automatically designates these allowances as consigned when the consigning entity enters an auction. The department of Ecology does not have control over the funds received from these allowances sold at auction. UTC retains oversight and jurisdiction for the use of these revenues, which are not deposited into state accounts, and are instead wired directly to the consigning entities from DB. The CCA IG recalculates and confirms the amount to be paid from DB is accurate and complete (step #2).

The day prior to the deposit, authorized Ecology Fiscal Office staff receive deposit amounts for each account from CCA IG staff, calculated in the step above. CCA IG will also include the Office of the State Treasurer (OST) so that they are notified of the expected amount, date, and time, that the wire transfer will be received. Carla contacts DB weeks before the expected transfer to ensure bank information maintained by DB is accurate and unchanged. Lars Andreassen, Agency Budget Director, also notifies Carla of the proper accounts to post deposit amounts. He monitors statutory requirements set by [RCW 70A.65](#) and appropriation amounts to ensure that amounts are recorded in the proper fund (26A, 26B, and 26C).

DB transfers state-owned auction proceeds to U.S. Bank for deposit after the completion and verification of each auction. As part of the financial settlement process, which begins when the auction results are published, seven days after the auction and continues another seven days (14 days post auction), DB will transfer funds from their accounts to the Washington Settlement Account and, when applicable in the future, to consigning entities. The "Financial Settlement Report" is a spreadsheet export that details all price and quantity information, including totals, and is generated 14 days after the auction by Mike Johnson, Cap-and-Invest Auctions Lead. This report is what the ECY uses to record revenue related to auctions.

### **How Transactions are Recorded in AFRS:**

Upon notification from U.S. Bank of the deposit, OST creates the ACH Accounts Receivable Report and the Wire Accounts Receivable Report. The CCA IG compares the financial settlement report to the AR report from OST to ensure the amounts to be received are correct. These fund totals from the financial settlement report are sent to Carla after the funds have been transmitted to OST. These funds are compared to what OST has recorded. Ecology's Fiscal Office downloads these reports from the OST TM\$ system and records the payment information, including dollar amounts and funds, on the A-8 Cash Journal, as long as they match the financial settlement report. The FA2 cashier prepares the A-8 entry in eHUB, and then it is submitted. An FA4 lead or Carla reviews the journal for accuracy and submits it to AFRS. The person who submitted to AFRS will review in AFRS and release it. At the same time the A-8 is submitted into AFRS, a file is created for OST in the integration from eHUB to AFRS and OST. ECY verifies in TM\$ that the A-8 file was received in TM\$ (**Key Control #2 - Valuation/Completeness**). The preparer will then print the journal entry header, line information, supporting TM\$ report, and CCA IG emails to be physically filed.

## State of Washington

The A-8 cash journal is transferred to and received by OST electronically the same day and they record their journal to deposit revenue as instructed by Ecology. Deposits into each applicable account must occur within 24 hours of when the auction proceeds are transferred from DB to U.S. Bank.

CCA IG publishes the Washington Auction Public Proceeds Report on Ecology's Auctions and Trading web page here: [Climate Commitment Act Notices and Reports](#) The report will be similar in format and content to CARB's [Auction Proceeds Summary](#).

### **Key Controls are as Follows:**

**Key Control 1 - Automated - (Valuation)** - The auction platform (ran by WCI) calculates all bid reports and results reports that drive the calculation of funds to be received from DB and then recorded by the ECY.

**Key Control 2 (Completeness)** - Ecology's Fiscal Office downloads the ACH/Wire Receivable reports from the OST TM\$ system (can take up to five days after the auction takes place) and records the payment information, including dollar amounts and funds, on the A-8 Cash Journal, as long as they match the financial statement settlement report (sent from the Auction Platform to DB and to ECY). The FA2 cashier prepares the A-8 entry in eHUB, and then it is submitted for review. An FA4 lead or Carla Clarey, Revenues Manager, confirms the amount is correct via email correspondence with DB and US Bank before submitting it to AFRS.

### **Noted Weaknesses are as Follows:**

None.

### **G.3.PRG - Licenses, Permits and Fees**

*Procedure Step:* Key Control #1 (Automated)

*Prepared By:* EJB, 8/12/2024

*Reviewed By:* CJG, 11/20/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To determine whether **Key Control 1 - Automated Software Calculation - (Valuation)** was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently

# State of Washington

during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - Auction Platform\]](#).

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

## State of Washington

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?



## State of Washington

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

## State of Washington

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

## State of Washington

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's*

# State of Washington

*testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

## **Computer Generated Reports:**

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

## **Electronic Approvals:**

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

## State of Washington

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

## State of Washington

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

## State of Washington

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

## State of Washington

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*



# State of Washington

## **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

## **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the **SOC Report Reliance** workpaper in the Store.

### **Automated Interfaces:**

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

## State of Washington

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.

If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.

## State of Washington

If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented

# State of Washington

in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

## **Manual vs. Automated Interfaces**

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

## State of Washington

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered “manual” since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient’s age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient’s name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or

## State of Washington

may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

- Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

- Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

# State of Washington

## Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.
----------------------

## **License, Permits & Fees CCA Auction Revenue - Valuation**

**Key Control 1 - Automated - (Valuation)** - The auction platform (ran by WCI) calculates all bid reports and results reports that drive the calculation of funds to be received from DB and then recorded by the ECY.

The understanding for this system is documented above in the "Controls - Auction Platform" step.

## **STEP 1: Understand Automated Key Control**

As detailed in the contract with WCI, ECY uses auction result reports produced by WCI's Auction Platform to record revenue related to each auction.

The Auction Platform calculates all bid reports based on the system's algorithm. See below for a detailed listing of the key reports derived form the Auction Platform:

Current Qualified Bidders Data - This report details the bidders and bidder types that qualify to enter each auction.

## State of Washington

Current Gather Bids - This report showed all bids made by entities participating in the auction.

(Current)Valid Price Points - This report showed which bids were qualified based on allowable allowances, bid guarantees, and holding limits.

Current Qualified Bids - This report showed additional information from the above report, and details out all bid edits made by the entity during the auction.

Current Demand Curve - This report showed all valid bids by entity that were won.

Current Distribution - This report showed all allotted allowances to bidders that were awarded allowances.

Final Results - This report shows the final results of the auction, including the settlement price, allowances won by each entity, and all funds expected to be received by each entity based on allowances won.

There are quarterly auctions in each fiscal year that use this Auction Platform and these reports are generated for each auction. These reports calculate the revenue amount to be recorded by the ECY. After the auctions are over, Ecology's Fiscal Office downloads ACH/Wire Receivable reports from the OST TM\$ system and records the payment information, including dollar amounts and funds, on the A-8 Cash Journal, as long as they match the financial settlement report. The FA2 cashier prepares the A-8 entry in eHUB, and then it is submitted. An FA4 lead or Carla reviews the journal for accuracy and submits it to AFRS (see [\[Key Control #2 \(Manual\)\]](#) for information on reporting these amounts).

Data is transferred immediately after the auction process has been completed, and ECY promptly recalculates all data provided in reports from the Auction Platform. Per discussion with ECY staff (as noted in the [\[Controls - Auction Platform\]](#) section), the process has yet to fail and WCI's algorithm has proven to work appropriately in each auction thus far (two auctions in 2023 and four in 2024). If there was a failure in the process, this would be caught by the code run by Scott Hancock, Senior Market Monitor (see the detail of the code run noted in the walkthrough in Step 2 below). The system will reject invalid bids before they can be made, and each qualified bidder will receive an error notification in real time.

### **STEP 2: Confirm and Test Automated Key Control:**

On July 15, 2024, we went to the ECY to perform a walkthrough of the CCA Auction Revenue process, and witnessed first hand the automated reports that come from the Auction Platform.

We reviewed all bids made in the auction and noted the settlement price was appropriately calculated (\$29.92/allowance). This was the amount reported in the public proceeds report available on the CCA's web site. We traced the lowest bid that won an allowance through each report, noting appropriate calculations had been made, along with the bid guarantees that were properly calculated in each report the auction platform produces. The total revenue to be recorded was \$157,379,200 which tied to the total released to the public on the Public Proceeds Report. See step 1 for all reports examined.

Scott Hancock (Senior Market Monitor) developed a source code that he runs (via RStudio) to confirm the bid holding limits, the qualified bidders report, the bid guarantees, the bid assignments (for bids that won an allowance and bids that did not win an allowance). Scott uses this source code to recalculate and verify that all information produced by the auction platform is accurate and calculates correctly. We witnessed Scott run



## State of Washington

this report the 2024 Q2 auction (June, 2024) and found no errors. We noted that the total number of allowances for sale, the total allowances won, and the bid price that all participants pay tied to the auction software data without error. This operates as a confirmation of the automated control.

Based on the above walkthrough, we noted that the controls in place appear to be operating as designed.

### **STEP 3: Understand General IT Controls**

Per discussion with the ECY team, there has not ever been errors or irregularities in the auction platform calculations.

Per discussion with Mike Johnson, Cap-and-Invest Auction Lead, ECY's CCA IG meets with WCI partner jurisdictions 2-3 times per week in regular meetings to discuss the maintenance, performance, and recommended updates & changes to the Auction Platform. These changes might include how different elements of the web page look, how Auction Platform Reports are executed, and the language, wording, and layout of each page.

**ECY has a structured policy in place for any edits or changes to be made to the algorithm. If ECY wants to make algorithm changes to edit the Auction reports, they reach out to the WCI to make these changes (General IT Control).** WCI makes the requested changes, and sends approval to ECY to test the changes via a mock auction. If the change is what ECY desires, they approve the change to be implemented for the next auction. WCI then implements these changes into the auction platform that is live for the next auction. ECY cannot make changes without confirmation emails with staff at WCI. Derek Nixon & Mike Johnson (Katie Murphy when Mike is out of office) are the only employees qualified to approve changes for WCI's review. Further changes are allowed to be made, but the same process must be repeated and tested by the entire ECY team. If any errors were caught in the algorithm (none thus far), the ECY would promptly reach out to the WCI to inquire as to what has occurred.

Mike mentioned that the auction platform has seen changes and updates released in the following times:

April, June, & September 2022.

February, April, July, and December 2023.

March 2024.

ECY is currently on their fifth version of the auction platform, and there have been 18 total changes that were fixed, tested, and approved for the current version of the auction platform. These tickets consist of updates or improvements related to password functionality (for bidders logging in to the platform), how digits are displayed in text boxes on the bidding page (size, alignment, and number of digits viewable at one time), how to "make public" instructional documents that are uploaded to the platform (FAQ and resources), specific changes to the French translation of an error message pop-up, and several tickets that were meant to confirm that the Nova Scotia jurisdiction has off-boarded appropriately and that Nova Scotia users no longer have access to data on the auction platform.

### **STEP 4: Confirm Key General IT Controls**

In order to confirm that **ECY has a structured policy in place for any edits or changes to be made to the algorithm**, we reached out to Derek and Mike and requested evidence of email communication about a recent change made to the Auction Platform algorithm. Mike responded

## State of Washington

with screen grabs from emails sent to Geeta Chaudhary, DevOps Engineer at WCI, on 7/25/2023 requesting changes to be made, and then the final implementation confirmation on 12/13/2023 for Platform Version 2.3 changes that were made in the software (Geeta confirmed), and that Mike had approved the changes after testing them in a controlled testing environment. This will suffice as a confirmation of the controls in place to make changes to the Auction Platform.

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **G.3.PRG - Licenses, Permits and Fees**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* EJB, 7/19/2024

*Reviewed By:* RKM, 12/17/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm **Key Control 2 (Completeness)**: Ecology's Fiscal Office downloads the ACH/Wire Receivable reports from the OST TM\$ system and records the payment information, including dollar amounts and funds, on the A-8 Cash Journal, as long as they match the financial statement settlement report. The FA2 cashier prepares the A-8 entry in eHUB, and then it is submitted for review. An FA4 lead or Carla Clarey, Revenues Manager, confirms the amount is correct via email correspondence with DB and US Bank before submitting it to AFRS in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

**Key Control 2 (Completeness)** - Ecology's Fiscal Office downloads the ACH/Wire Receivable reports from the OST TM\$ system (can take up to five days after the auction takes place) and records the payment information, including dollar amounts and funds, on the A-8 Cash Journal, as long as they match the financial statement settlement report (sent from the Auction Platform to DB and to ECY). The FA2 cashier prepares the A-8 entry in eHUB, and then it is submitted for review. An FA4 lead or Carla Clarey, Revenues Manager, confirms the amount is correct via email correspondence with DB and US Bank before submitting it to AFRS.

The understanding for this system is documented above in the [\[Controls - Auction Platform\]](#) step.

## **1. Confirmation of Key Manual Control:**

We observed the revenue recognition entry by examining all preparation documents provided to us by Carla Clarey, Revenue Receivables Manager, from the April auction (Document number 461X1860, JV#CJ-000259619, processed 4/2/2024). We reviewed the AFRS cash receipts journal summary detailing the total amount from auction, the cash receipts journal summary, the cash journal deposit detail, the cash journal receipt by remitter, the cash flow desk wire master file, confirmation email between Carla and Katie Murphy, Cap-and-Invest Market Planner, detailing the revenue to be recorded as a result from the April auction by reviewing the financial settlement report, and the confirmation email between ECY's cashing department and DB showing the wire transfer has been released. We determined the control is in place.

## **Noted Weaknesses are as follows:**

None.

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **G.3.PR.G - Licenses, Permits and Fees**

*Procedure Step:* Risk Assessment

*Prepared By:* EJB, 9/9/2024

*Reviewed By:* CJG, 11/20/2024

# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

*General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

*Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

## State of Washington

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

## State of Washington

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation - IR for Valuation is **moderate**

Completeness– IR for completeness is **low**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**Auction Platform Software** – Valuation - **MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.



## State of Washington

**eHub/AFRS** – Completeness - **MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation - Mod - RMM cannot be higher than IR.

Completeness - Low - RMM cannot be higher than IR.

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

Valuation:

Recalculate the total revenue to be recorded from the Final Results tab from the Auction Platform by multiplying the auction settlement price by the total number of allowances sold for each auction in 2024.

Tie the revenue to be recorded from the Final Results tab from the auction platform bid report to the public proceeds statement for each auction in 2024.

Tie the public proceeds report to what is recorded in eHub and then subsequently reported in AFRS for each auction in 2024.

Completeness:

Obtain the ACH transaction report or evidence of cash receipt of the Q4 auction revenue and ensure the total amount received ties to the receivable amount recorded at year end.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **G.3.PR.G - Licenses, Permits and Fees**

*Procedure Step:* Substantive Test

*Prepared By:* EJB, 9/17/2024

*Reviewed By:* RKM, 12/10/2024

# State of Washington

## Purpose/Conclusion:

### **Purpose:**

To determine whether all revenues relating to the period were reported as of 6/30/2024 (Completeness).

To determine whether revenues were reported at properly valued or calculated amounts (Valuation).

### **Conclusion:**

We determined revenues relating to the period were reported as of 6/30/2024.

We determined revenues were reported at properly valued or calculated amounts.

## Testing Strategy:

The following is a list of **considerations** for testing the completeness assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

- Identify expected revenue streams based on understanding of fund activities and scan to see if revenue is reported for all such streams.

- Follow up on any unexpectedly missing streams.

- Identify new revenues (ex: new grants or programs) and follow up to verify that expected revenues have been reported.

- Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

- If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

- Trace selected or sampled revenues from source documents to accounting records.

*Source documents may consist of billing, fine, or fee records. Or it may consist of service records that imply a billing, such as license or permit issuance.*

- Perform a multi-year trend of revenues and follow up on unexpected decreases.

- Search for manual journal entries that debit (decrease) revenues. Consider testing if any risk indicators are noted.

# State of Washington

## **Cut-Off**

Test transactions recorded in the next period to determine whether the revenue should have been recorded in the current period.

*Transactions recorded at the beginning of the next period would generally be considered at highest risk of being improperly shifted to that future period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields. If the population is large, consider stratifying to either scan and select or test 100% of all large value transactions combined with a lower assurance sample for small dollar transactions.*

## **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Calculation**

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

## **Realizable Value**

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

## **Estimation / Recognition**

Review calculation and support for assumptions of any estimated revenues.

# State of Washington

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

**Property Tax Revenues** - see separate step

Guidance/Criteria:

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

**BARS [3.6.11](#) Suspense Funds**

Record of Work Done:

**Per [RCW 70A.65.100](#): Auctions of allowances (Contingent Expiration Date)**, section 9, "records containing the following information are confidential and are exempt from public disclosure in their entirety: a) Bidding information identified in subsection (8) of this section; (b) information contained in the secure, online electronic tracking system established by the department pursuant to RCW 70A.65.090(6); (c) Financial, proprietary, and other market sensitive information as determined by the department that is submitted to the department pursuant to this chapter; (d) Financial, proprietary, and other market sensitive information as determined by the department that is submitted to the independent contractor or the financial services administrator engaged by the department pursuant to subsection (3) of this section; and (e) Financial, proprietary, and other market sensitive information as determined by the department that is submitted to a jurisdiction with which the department has entered into a linkage agreement pursuant to RCW 70A.65.210, and which is shared with the department, the independent contractor, or the financial services administrator pursuant to a linkage agreement.

**Due to the above, we will not be documenting any specific amounts that we examine that are not reported in the public proceeds report. However, we will confirm the allowance settlement price was calculated correctly. See testing at: [[CCA Revenue Workbook](#)].**

## **Substantive tests performed to meet the Completeness assertion:**

Completeness:

Obtain the ACH transaction report or evidence of cash receipt of the Q4 auction revenue and ensure the total amount received ties to the receivable amount recorded at year end.

We observed the revenue recognition entry by examining all preparation documents provided to us by Carla Clarey, Revenue Receivables

## State of Washington

Manager, from the June auction (JV#461X2360 processed 7/2/2024). We reviewed the AFRS deposit Cash Receipts Journal Summary, as well as the cash receipts summary detailing the cash receipt on 7/2/2024 of the Q4 Auction results. The revenue recorded tied to the receivable reported, as well as the final settlement auction report tab and the public proceeds report. This test was met without error.

### **Substantive tests performed to meet the Valuation assertion:**

Valuation:

Recalculate the total revenue to be recorded from the Final Results tab from the Auction Platform by multiplying the auction settlement price by the total number of allowances sold for each auction in 2024 (four quarterly auctions and 2 APCR auctions).

Tie the revenue to be recorded from the Final Results tab from the auction platform bid report to the public proceeds statement for each auction in 2024.

Tie the public proceeds report to what is recorded in eHub for each auction in 2024.

The testing procedures are as follows:

Test A: We tested that the auction settlement price was calculated correctly by looking at the Auction Reports. The auction reports detailed the total amount of bids made by each entity participating in the auction. From this report, I was able to filter by bid amount from largest to smallest. I was then able to see the lowest bid that won an allowance. This bid is the auction settlement price that all participants pay at the conclusion of the auction.

Test B: We reviewed the Auction Results Tab which detailed the amount of allowances that were sold in total at the auction. We were able to recalculate the total amount of revenue due to the ECY by multiplying the auction settlement price by the total number of allowances sold.

Test C: The Final Auction Results tab showed the settlement price (auditor performed recalculation in Step A) and the total revenue to be recorded at ECY (recalculated in Step B), which we were able to tie to the public proceeds report available on the ECY's website. See testing workpaper for the JV#'s, as well as the date the funds were deposited.

Test D: The public proceeds reports then tied to each journal voucher recorded in eHub for each auction. This in turn, was recorded correctly in AFRS.

The above tests were all met without error.

### **H.1.PRG - Tax Collections for Other Governments**

*Procedure Step:* Summary & Conclusion

*Prepared By:* CJM, 11/20/2024

*Reviewed By:* RKM, 11/21/2024

# State of Washington

Purpose/Conclusion:

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the [Permanent File](#) by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

Is information precise enough to catch if misstatements exceeded the tolerable level?

Is information detailed enough to conclude on whether or not there were misstatements?

## State of Washington

Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?

How did misstatements occur and how often might they occur again in the population?

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

# State of Washington

## **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **H.1.PRG - Tax Collections for Other Governments**

*Procedure Step:* Understanding of Line Item

*Prepared By:* CJM, 6/3/2024

*Reviewed By:* RKM, 6/11/2024

Purpose/Conclusion:

#### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

#### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

#### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.



## State of Washington

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

# State of Washington

## **(1) Prior Audit Exceptions:**

There were no exceptions noted in prior audit.

## **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

Fund 034 - Local Sales and Use Tax - State share (6.5% per statute) and Add-on (decided by city and county)

Fund 01T - Local Leasehold Excise Tax

Fund 16C - Real Estate and Property Tax Administration Assistance

Fund 17A - County Enhanced 911 Excise Tax

Fund 768 - Local Real Estate Excise Tax (REET)

Fund 797 - Local Tourism Promotion Tax

On May 8, 2024, we met with Jason Hartwell, Tax Admin Manager, and on May 14, 2024, we met with Ayano Faasumalie, Revenue and Finance Rep Coordinator, to discuss any changes to the transactions and process for this line item in relation to the prior year. For fiscal year 2024, Business and Financial Services (B&FS) makes manual quarterly adjustments in AFRS until automated entries can be implemented in Automated Tax and Licensing Administration System (ATLAS). This quarterly adjustment process is similar to prior years. Per inquiry with B&FS staff, we also noted the composition of the balance remains the same as the prior year.

Upon review of the line item lead sheet for FY23 balances, we noted 98% of the balance is collections for fund 034, local sales and use tax. We expect the FY24 balance to remain similar based on our discussion with the agency. Therefore, we will focus our control understanding and testing on the local sales and use tax portion of the balance.

## **(3) Updates to Significant Account Matrix:**

No updates to the Significant Account Matrix is needed.

## **H.1.PR.G - Tax Collections for Other Governments**

*Procedure Step:* Controls - ATLAS

*Prepared By:* CJM, 6/4/2024

*Reviewed By:* RKM, 6/11/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant

## State of Washington

deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- Initiation:* How are transactions initiated?
- Authorization:* How are transactions and accounting record maintenance authorized?
- Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

# State of Washington

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Material Balance(s) and Assertions**

Internal controls in the Automated Tax and Licensing Administration System (ATLAS) address the following balance(s):

**Tax Collections for Other Governments** - Custodial Funds

For the following assertions:

**Classification** - There is a risk that revenues are incorrectly classified as local when they were actually state taxes.

**Valuation** - There is a risk that taxes were incorrectly valued (wrong tax rate).

**Completeness** - There is a risk that not all taxes collected on behalf of local governments have been identified.

## **Gain an Understanding of Internal Controls**

We met with Jason Hartwell, Tax Administration Manager, and Courtney Tornquist, Systems Specialist, on May 8, 2024 to discuss controls related to the Payments of Taxes to Other Governments.

Local Tax Rates

## State of Washington

Counties, cities, and local tax codes have the authority to assess local taxes in addition to the state's regular 6.5% sales and use tax (use tax is the same rate as sales tax, taxpayers would pay this when purchasing a television in Oregon for example). These taxes are regulated by ordinances or resolutions set by the local governments. Each jurisdiction has a collection agreement on file with DOR that includes the administration fee charged (if applicable) and how refunds and redistributions are handled. When a jurisdiction passes a resolution or ordinance to collect a new tax, they must provide DOR with written notification, a copy of certified election results and a copy of the ordinance or resolution. The jurisdiction must provide the documentation at least 75 days before the effective date (January 1, April 1, and July 1). Taxpayer Account Administration (TAA) has an Excise Tax Examiner (ETE) on the local tax team that will monitor and review election result documentation quarterly to verify if any new taxes or rates have passed.

### Local Tax (LT) Rate Testing in ATLAS

The process for updating the local tax rates is:

1. A LT manager receives documentation from a jurisdiction indicating they have passed a resolution/ordinance. Once the documents are reviewed/verified, the manager puts the changes on a spreadsheet and emails that spreadsheet to the LT system specialist.
2. In a test environment, a programmer updates rate tables as necessary. This environment is verified by reviewing the rates in the Automated Tax and Licensing Administration System (ATLAS) and from various ad hoc reports. Then the changes are moved to the production environment.
3. A programmer will then make system application changes in the test environments. The LT system specialist file test batches (tax returns) for this environment and ensures that they post and calculate properly. ATLAS is then verified for proper accumulation and distribution. Then the application changes are moved to the production environment.

The LT system specialist conducts testing in production to ensure accumulation and distribution amounts are accurate and only local tax codes are included prior to distribution to jurisdictions. TAA will also verify local tax calculations using the new rates on a monthly basis. Money is not distributed to local governments by OST until TAA verifies the data in ATLAS (**Key Control 1 - Valuation/Classification - Manual**). Distributions usually occur the following month after tax returns are due. This allows TAA to work through any identified issues.

### Calculation of Local Sales and Use Tax

Businesses are assigned a location code in ATLAS. The location codes feed back to the jurisdiction for tax collection and local taxes accumulate to the reported locations based on the taxes imposed in each jurisdiction. Filers are required to submit Excise Tax returns where local tax data is captured in ATLAS. The Combined Excise Tax Return form requires businesses input a location name and location code when reporting local sales tax collected. Based on the information input by the taxpayer, ATLAS captures the total taxes collected and sums it up by the type of local tax by location code (**Key Control 2 - Valuation - Automated**). Local sales and use tax are calculated and recorded within ATLAS similar to the other types of tax revenues reviewed at [\[Retail Sales and Use and B&O Taxes\]](#). If a return is filed with a wrong location code or any errors, the return will error out in the system and will not be recorded until it is manually reviewed and resolved by a TAA examiner. The error will go into a work queue.

# State of Washington

task that is pulled and reviewed by the examiners. If corrections are required, they will make the adjustment and save it in the system.

Local Sales and Use Tax are not the State's and are only collected and distributed by DOR on behalf of the local jurisdictions. When a taxpayer submits a payment, DOR initially uses ATLAS to record the amount in the Suspense Account within the Office of the State Treasurer (OST). The money is held in trust and redistributed monthly by OST. When the payment is applied to the tax return, ATLAS generates a JV to record a "Due to Other Funds" (Short-Term) in AFRS. On the last day of the month DOR enters a JV to reclassify the amount to be distributed by OST as "Due to Other Governments" (MC).

## **How Transactions are Recorded in AFRS:**

### Gross Receipts Accrual

For monthly filers, Excise Tax returns for June activity are due July 25th. For quarterly filers the tax returns for the 4th fiscal quarter (April, May, and June) are due July 31st. At June 30th, tax has been collected by businesses (taxpayers), from their customers, for sales occurring during the month of June; however, they are not required to file their tax returns and turn over the amount collected on their June sales until July 25th, when the June tax return is due. The Due to Other Governments portion is the amount collected by the tax payer for their location (i.e. city) and then sent to DOR when the taxpayer files and remits their monthly taxes (state and local). After year end, an AFRS entry is made to recognize these revenues and due to other governments in the proper accounting period (current year under audit). This is because at June 30th these revenues will not have been recorded (as received or as a receivable) due to Excise Tax returns not being received by year-end.

In August, B&FS runs a report (B9901FI1Y Gross Receipts Accrual Report) in ATLAS to pull data of June excise tax returns and the 4th fiscal quarter (April, May, and June) returns received from July 1st to August 15th. The Department estimates that 90 to 96% of the June returns and the 4th fiscal quarter (April, May, and June) returns are received by the time the report is run and therefore included on the report. Using this report, an AFRS entry is made to show the June returns received as a June 30th receivable and accrued revenue. The accrued revenue is an estimated amount of tax returns that will be paid within 12 months of the fiscal year end.

### Adjusting Entries

We met with Ayano Faasumalie, Revenue and Financial Reporting Coordinator, on May 14, 2024 to discuss the process for recording all tax collections and distributions for FY2024. Due to guidance received from OFM, DOR changed their reporting of local sales and use tax starting in FY21. This change resulted in all collections and distributions of taxes being recorded as additions and deductions in the Fiduciary Statement of Net Position. ATLAS already prepares monthly journal entries to record excise tax receivable, accrued revenue, and unavailable revenue. After ATLAS creates JVs, B&FS has 6 business days to review the JVs before it is transmitted to AFRS. The receivable and revenue calculations are then reversed out for the beginning of the next month. At the end of each month, Revenue Accounting will also prepare a monthly JV to record the distributions of taxes. Revenue Accounting will retrieve a report from the Treasury Management System (TM\$) that shows how much OST distributed to local jurisdictions. Based on this report, a JV is recorded in ATLAS to match the distribution from TM\$. If the JV does not match with the OST reports, the transaction will show up on DOR's unbalanced in-process report.

## State of Washington

Using the monthly JVs created by Revenue Accounting and the ATLAS automated JVs, the Revenue and Financial Reporting Coordinator prepares an adjusting entry to record all collections and distributions for each quarter. The Revenue and Financial Reporting Coordinator runs a Webi report for all data included in GL 5152 (Due To Other Governments) for the quarter to determine the amounts to be reported as collections (GL 3205) and distributions (GL 6505). She separates the Webi query into different excel tabs based on funds. For each fund and subsidiary account, she further separates the amounts into the following:

- Collection for Distribution
  - From the prior quarter to be distributed in the current
  - From the current quarter to be distributed in the current
- Distributions
- Collection for Future Distribution

The amounts are summarized in the quarterly Activities Summary by Fund spreadsheet and highlighted to track exactly where the figures came from. Based on the summary, the Revenue and Financial Reporting Coordinator prepares the journal voucher to record collections and distributions. The final JV is reviewed and approved by an Accounting Manager, to ensure all collections and distributions are recorded for the quarter (**Key Control 3 - Completeness - Manual**).

### Key controls are as follows:

**Key Control 1 - Valuation/Classification - Manual** - The Local Tax System Specialist conducts testing in production to ensure accumulation and distribution amounts are accurate and only local tax codes are included prior to distribution to jurisdictions.

Taxpayer Account Administration (TAA) will also verify local tax calculations using the new rates on a monthly basis.

**Key Control 2 - Valuation - Automated** - Based on the location code entered by the tax filer, ATLAS calculates the local sales and use taxes due.

**Key Control 3 - Completeness - Manual** - The Revenue and Financial Reporting Coordinator prepares an adjusting entry to record all collections and distributions for each quarter. The final JV is reviewed and approved by the Accounting Manager to ensure all collections and distributions are recorded for the year and match.

### Noted Weaknesses are as Follows:

None.

### H.1.PRG - Tax Collections for Other Governments

*Procedure Step:* Key Control 1 (Manual)

*Prepared By:* CJM, 6/4/2024



# State of Washington

Reviewed By: RKM, 6/11/2024

Purpose/Conclusion:

**Purpose:**

To confirm whether Taxpayer Account Administration verifies accumulation data in ATLAS prior to distribution to local governments (Key Control 1 for ATLAS) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated"*

## State of Washington

*step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider*

## State of Washington

*whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 1 Valuation/Classification - Manual** - The Local Tax System Specialist conducts testing in production to ensure accumulation and distribution amounts are accurate and only local tax codes are included prior to distribution to jurisdictions. Taxpayer Account Administration (TAA) will also verify local tax calculations using the new rates on a monthly basis.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

On May 8th, 2024, we spoke with Jason Hartwell, Tax Administration Manager for Local Tax, and Courtney Tornquist, System Specialist, about reconciliations performed on a monthly basis to ensure local tax accumulated per jurisdiction are accurate. Courtney performs the quarterly tax rate change testing as well as the monthly production testing. Courtney stated the monthly production testing is done on a sample basis to verify the accumulations are accurate before OST distributes the funds back to the local jurisdictions. During the monthly testing, she will also include jurisdictions that had recent changes. During the meeting they provided a walkthrough of the March 2024 production testing. The March testing included the following jurisdictions:

4 - Chelan

# State of Washington

9 - Douglas  
28 - San Juan

Each county selected for testing has its own individual tab and data feeds into the summary table where recalculations are compared to accumulation amounts from ATLAS. Any variances not attributed to rounding are investigated and corrected if needed. We noted the system specialist identified a few variances between ATLAS and the recalculated accumulation. The largest variances were reconciled and were identified as variances due to the payment timing of rural state shared tax. We noted the variances were reduced to reasonable differences (no more than 0.5% of variance for any jurisdiction). ***No issues noted.***

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **H.1.PRG - Tax Collections for Other Governments**

*Procedure Step:* Key Control 2 (Automated)

*Prepared By:* CJM, 10/16/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion:
---------------------

## **Purpose:**

To determine whether ATLAS calculates the local sales and use taxes due based on the location code entered by the tax filer (Key Control 2 for

## State of Washington

ATLAS) was in place in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [Controls - ATLAS].

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

*g monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

# State of Washington

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

## State of Washington

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient*

## State of Washington

*evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.



# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Information Technology](#) Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

#### Manual vs. Automated Interfaces

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

## State of Washington

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program,

## State of Washington

also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An "**electronic signature**" can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A "**digital signature**" is a legal signature with a formal certification process that documents who approved the document and ensures the

# State of Washington

document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control 2 Valuation - Automated** - Based on the location code entered by the tax filer, ATLAS calculates the local sales and use taxes due.

## **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

## **STEP 2: Confirm and Test Automated Key Control:**

We obtained tax return information from ATLAS for a sample of taxpayers that paid local sales and use taxes during FY24 and re-performed the tax calculations. See testing at [[Local Tax Collection Distribution Testing - CONFIDENTIAL](#)]. Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

## **STEP 3: Understand General IT Controls**

On May 8, 2024, we met with Jason Hartwell, Tax Administration Manager, and Courtney Tornquist, IT Business Analyst, to gain an understanding of the general IT controls for ATLAS. Maintaining and updating the Department of Revenue's (DOR) Automated Tax and Licensing Administration System (ATLAS) is a large undertaking that requires coordination across multiple areas of the agency. Various division staff routinely prepare change requests (known as SQRs) to correct defects, update, or create new system functionality and configuration. SQRs are the mechanism used to facilitate the process and ultimately become the system of record for the development activities. SQRs must be reviewed and approved via a workflow process within the Fast Code Repository (FCR) environment before its implemented into ATLAS (**General IT Control 1**). Formulas and calculating factors are stored in ATLAS within a programming table and require a SQR to update an automated calculation. The calculations are triggered by the Tax Filer when they submit a tax return. When errors occur during the SQR process an alert will show in the workflow process and

# State of Washington

a developer will be assigned to correct the error.

## **SQR Workflow Process**

On May 23, 2024, we met with Lucas Kenall, ATLAS Development & Technology Services Manager. When a change to tax rates are needed a SQR submitter creates a request. A Change Manager reviews the request to ensure it is necessary and filled out correctly. When the request is approved a developer is assigned. The requested changes are made in a testing environment to ensure they are implemented correctly without affecting the active ATLAS rates. When the testing is complete the SQR is placed into staging where it is reviewed to ensure it will function correctly. Approvals from 2 members ATLAS development and Technology Services Team are needed to complete the process. When the staging is complete the SQR is passed to the migration step where it will be automatically deployed to ATLAS during non-business hours. Weekly the ATLAS services team ensures that migrations complete with the proper approvals by running a Migration Audit Report that show all migration statuses and approvals. Once the migration has completed successfully the SQR is closed.

## **STEP 4: Confirm Key General IT Controls**

**General IT Control 1:** SQRs must be reviewed and approved via a workflow process within the Fast Code Repository (FCR) environment before its implemented into ATLAS.

On May 8, 2024, Courtney Tornquist, System Specialist, provided us with screenshots of SQR 15578: Local Tax-Quarter 1 2024 changes. We reviewed the SQR workflow to ensure that each step in the process was signed off and approved before moving on to the required next step. The SQR was initiated by Jason Hartwell on October 18, 2023. The SQR was assigned to Courtney Tornquist. We reviewed the workflow logs for the SQR and noted that each step had notes and approvals showing adequate review. The SQR process was closed on March 12, 2024. **No issues noted.**

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **H.1.PR.G - Tax Collections for Other Governments**

*Procedure Step:* Key Control 3 (Manual)

*Prepared By:* CJM, 6/4/2024

*Reviewed By:* RKM, 6/11/2024

## State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm an adjusting entry to record all collections and distributions for each quarter is prepared (Key Control 3 for ATLAS) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

## State of Washington

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

## State of Washington

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 3 - Completeness - Manual** - The Revenue and Financial Reporting Coordinator prepares an adjusting entry to record all collections and distributions for each quarter. The final JV is reviewed and approved by the Accounting Manager to ensure all collections and distributions are recorded for the year and match.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

#### **Quarterly Adjusting Entry Review**

We obtained AFRS journal voucher number 14030250. We noted the explanation of the entry was "To record additions and deductions for Fund 01T, 034, 16C, 17A, 768, 797 for Qtr 1, FY 2024 (July - September, 2023)". Per the line item lead sheet, we noted the majority of the balance is included in fund 034, Local Sales and Use Tax, which is where we focused our control review and testing. We noted the total amount of local sales and use tax collected account was \$1,979,599,134. The collection amounts are based on the monthly JV entries automatically created by ATLAS. We agreed the amounts reported in the JV to a summary of all monthly JVs in quarter 1 from ATLAS. The total collection of local sales and use tax that was distributed in 2024 totaled to \$1,979,599,134. Amounts tie without exception. The JV was prepared by Ayano Faasumalie, Revenue and Financial Reporting Coordinator, on October 23, 2023 and reviewed by Binh Vu, Accounting Manager, on October 23, 2023. ***No issues noted.***



# State of Washington

## Noted Weaknesses are as follows:

None

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX-** We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW – Test of Key Manual Control:**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at maximum.

## **H.1.PRG - Tax Collections for Other Governments**

*Procedure Step:* Risk Assessment

*Prepared By:* CJM, 7/25/2024

*Reviewed By:* RKM, 8/9/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

1. Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to a material misstatement, assuming that there are no related controls. Inherent risk can*

## State of Washington

*be thought of as the "threat" of misstatement. Inherent risk exists independently of control risk (the level of threat exists independent of the level of vulnerability to threats). Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*· Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## State of Washington

2. Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and testing (if applicable). If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*In order to set control risk to LOW, general controls would also need to be tested to provide evidence of the consistent operation of automated controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body.*

***All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

3. Assess the risk of material misstatement for each relevant assertion for each material line item. The risk of material misstatement is a combination of the auditor's separate assessment of inherent and control risk.

*The Risk of Material Misstatement is a combined assessment of inherent and control risk based on auditor's judgment. If inherent and control risk are assessed differently, it is a matter of professional judgment as to whether the combined assessment is moderate or if one factor outweighs the other.*

4. Design a substantive testing strategy that addresses the relevant assertion in all significant transaction streams included within the material line item.

*In addition to identifying what to audit (material balances) and what to audit for (relevant assertions), planning has also identified how much to audit (risk of material misstatement). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:
----------------------

**(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

**Classification - Moderate**

**Completeness - Moderate**

**Valuation - Moderate**

**(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**Automated Tax and Licensing Administration System (ATLAS) -**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

**(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**Classification - Mod**

**Completeness - Mod**

**Valuation - Mod**

**(4) Testing Strategy:**

# State of Washington

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

**Classification** - We will review a sample of registered taxpayers and ensure tax types are properly categorized as Local Sales and Use Taxes.

We will review quarterly JVs to ensure amounts reported as collections/distributions for other governments are only local taxes.

**Completeness** - We will use the same sample of registered taxpayers as above, review ATLAS for a filed return, and trace revenue to the accumulation GL within ATLAS and to AFRS. We will also review quarterly JVs to ensure monthly automated accumulations within ATLAS were included in the JV and we will review quarterly collection/distribution JVs to ensure that collections and distributions match and are recorded at accurate values.

**Valuation** - We will recalculate taxes paid for the same sample of registered taxpayers as above, to ensure taxes are recorded at proper values and are based on local tax rates and not state tax rates.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## H.1.PRG - Tax Collections for Other Governments

*Procedure Step:* Substantive Test

*Prepared By:* CJM, 10/16/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion.
---------------------

### **Purpose:**

To determine whether financial statements properly classify local tax collections (Classification).

To determine whether all local tax collections relating to the period were reported (Completeness).

To determine whether local tax collections were reported at properly valued or calculated amounts (Valuation),

### **Conclusion:**

We determined:

Financial statements properly classify local tax collections (Classification).

All local tax collections relating to the period were reported (Completeness).

Local tax collections were reported at properly valued or calculated amounts (Valuation).

# State of Washington

## Testing Strategy:

The following is a list of **considerations** for testing the completeness assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Identify expected revenue streams based on understanding of fund activities and scan to see if revenue is reported for all such streams.

Follow up on any unexpectedly missing streams.

Identify new revenues (ex: new grants or programs) and follow up to verify that expected revenues have been reported.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Trace selected or sampled revenues from source documents to accounting records.

*Source documents may consist of billing, fine, or fee records. Or it may consist of service records that imply a billing, such as license or permit issuance.*

Perform a multi-year trend of revenues and follow up on unexpected decreases.

Search for manual journal entries that debit (decrease) revenues. Consider testing if any risk indicators are noted.

## Cut-Off

Test transactions recorded in the next period to determine whether the revenue should have been recorded in the current period.

*Transactions recorded at the beginning of the next period would generally be considered at highest risk of being improperly shifted to that future period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields. If the population is large, consider stratifying to either scan and select or test 100% of all large value transactions combined with a lower assurance sample for small dollar transactions.*

## Detail Roll-up

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at*

# State of Washington

*the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Calculation**

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

## **Realizable Value**

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

## **Estimation / Recognition**

Review calculation and support for assumptions of any estimated revenues.

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

The following is a list of **considerations** for testing the classification assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Classification between Line items**

Scan revenue streams or types to evaluate whether they appear reasonable in relation to the line item description. Follow-up on any unexpected results with accounting research to determine correct classification.

Select or sample revenues from high risk populations and review supporting documentation that demonstrates correct classification of revenues.

Search for manual journal entries that re-classify existing revenue balances (transaction is a debit and credit to different revenue accounts). Consider testing if any risk indicators are noted.

## **Classification between Opinion Units**

## State of Washington

Search for manual journal entries that transfer revenues from one opinion unit to another without recording a balance sheet transaction, other than a direct charge to fund balance (debit and credit to revenue and fund balance for each opinion unit, respectively). Consider testing if any risk indicators are noted.

Scan revenue streams or types by fund and evaluate whether revenue streams or types appear reasonable in relation to the activities of the fund. Follow-up on any unexpected results with accounting research to determine correct classification.

Guidance/Criteria:

**BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

**BARS [3.6.11](#) Suspense Funds**

**BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

**BARS [1.5](#) Determining Operating/Nonoperating/Revenues/Expenses in Proprietary Funds**

**BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

**BARS [3.6.11](#) Suspense Funds**

**BARS [3.6.13](#) Utility Tax (*applies only to cities*)** - should be accounted for as a revenue in the general fund (3164000) and expenditure in the utility fund (53P0040), if the utility passes the tax on to its customers then the additional charges should be recognized as revenue (343P000) directly in the utility fund not in the general fund

Record of Work Done:

### **Tax Collections for Other Governments Testing Coverage**

We reviewed the line item leadsheet [[Line Item Lead Sheet](#)] and noted Fund 034 - Local Sales & Use Tax accounts for the majority of all tax collections for other governments. We determined focusing our testing on Fund 034 collections would provide sufficient coverage over the balance to meet the relevant assertions. See testing details below.

### **Substantive tests performed to meet the Completeness assertion:**

We obtained a list of all active taxpayers that paid local sales and use taxes as of 6/30/2024 and randomly selected a sample of 30 taxpayers for various periods to ensure the return was accurately filed and posted to AFRS. Jason Hartwell, Tax Administration Manager, provided a screenshot of all taxpayers' tax returns entered in ATLAS as well as their payment of the calculated taxes. We reviewed the return for the selected taxpayers



## State of Washington

in ATLAS to ensure a return was filed and payments were received for the entire amount recorded in the return. See testing performed at [[Local Tax Collection Distribution Testing - CONFIDENTIAL](#)]. **No issues noted.**

Business and Financial Services makes an adjusting entry to record local tax collections as tax collections for other governments and tax payments to other governments to comply with GASB 84 regulations on a quarterly basis. When payments for local taxes are collected, ATLAS automatically accumulates revenues to the appropriate fund and GL in a monthly JV. The quarterly collection/distribution JVs includes the monthly accumulation JV activity and moves 5152 - Due to Other Governments to the revenues and expenditures GL (32XX and 65XX). We reviewed each quarter's adjusting JV to ensure:

- All automated ATLAS JVs are recorded and in the proper period
- Quarterly JV amounts only include local taxes
- Collections and Distributions for each month match

We noted the quarterly JVs were complete based on the testing above. See testing at [[Quarterly Collection Distribution JVs](#)]. **No issues noted.**

### **Substantive tests performed to meet the Valuation assertion:**

Using the same randomly selected sample of 30 taxpayers, as mentioned above, we recalculated taxes paid based on local tax rates to ensure that revenues related to local sales and use tax were valued at proper amounts and based on local tax rates and were not related to state tax revenues. Jason Hartwell, Tax Administration Manager, provided a screenshot of all selected taxpayers' tax returns entered in ATLAS. We obtained the local sales and use tax rates for each selected period from the DOR website. Based on the taxable amount in the tax returns, we recalculated the collected local sales and use tax. Any differences noted were small rounding errors. We determined all selected local sales and use tax collections/distributions were reported at properly valued and calculated amounts. See testing performed at [[Local Tax Collection Distribution Testing - CONFIDENTIAL](#)]. **No issues noted.**

### **Substantive tests performed to meet the Classification assertion:**

Using the same randomly selected sample of 30 taxpayers, as mentioned above, we tested to ensure that collections/distributions were properly categorized as Local Sales and Use Taxes. Jason Hartwell, Tax Administration Manager, provided a screenshot of all selected taxpayers' tax returns entered in ATLAS. We obtained the local sales and use tax rates for each selected period from the DOR website. We reviewed the ATLAS tax returns to ensure that only local agencies were included and selections were properly categorized as local city or county taxes collected as use, sales tax, or deferred sales tax. We determined all selected taxpayers were properly categorized and reported. See testing performed at [[Local Tax Collection Distribution Testing - CONFIDENTIAL](#)]. **No issues noted.**

Business and Financial Services makes an adjusting entry to record local tax collections as tax collections for other governments and tax payments to other governments to comply with GASB 84 regulations on a quarterly basis. When payments for local taxes are collected, ATLAS automatically accumulates revenues to the appropriate fund and GL in a monthly JV. The quarterly collection/distribution JVs includes the monthly accumulation JV activity and moves 5152 - Due to Other Governments to the revenues and expenditures GL (32XX and 65XX). We reviewed each quarter's

# State of Washington

adjusting JV to ensure:

Quarterly JV amounts only include local taxes

We noted the quarterly JVs were classified appropriately based on the testing above. See testing at [\[Quarterly Collection Distribution JVs\]](#). ***No issues noted.***

## H.2.PRG - Payments of Taxes to Other Governments

*Procedure Step:* Summary & Conclusion

*Prepared By:* CJM, 11/20/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting*

## State of Washington

*the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the **Permanent File** folder or assessment of control risk?
  - If circumvention, the **Management Override of Controls** step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in*

## State of Washington

*the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

#### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

#### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **H.2.PRG - Payments of Taxes to Other Governments**

*Procedure Step:* Understanding of Line Item

*Prepared By:* CJM, 6/3/2024

*Reviewed By:* RKM, 6/11/2024

# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or

## State of Washington

reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria:

Record of Work Done:

#### **(1) Prior Audit Exceptions:**

There were no exceptions noted in prior audit.

#### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

Fund 034 - Local Sales and Use Tax - State share (6.5% per statute) and Add-on (decided by city and county)

Fund 01T - Local Leasehold Excise Tax

Fund 16C - Real Estate and Property Tax Administration Assistance

Fund 17A - County Enhanced 911 Excise Tax

Fund 768 - Local Real Estate Excise Tax (REET)

Fund 797 - Local Tourism Promotion Tax

On May 8, 2024, we met with Jason Hartwell, Tax Admin Manager, and on May 14, 2024, we met with Ayano Faasumalie, Revenue and Finance Rep Coordinator, to discuss any changes to the transactions and process for this line item in relation to the prior year. For fiscal year 2024,

# State of Washington

Business and Financial Services (B&FS) makes manual quarterly adjustments in AFRS until automated entries can be implemented in Automated Tax and Licensing Administration System (ATLAS). This quarterly adjustment process is similar to prior years. Per inquiry with B&FS staff, we also noted the composition of the balance remains the same as the prior year.

Upon review of the line item lead sheet for FY23 balances, we noted 98% of the balance is collections for fund 034, local sales and use tax. We expect the FY24 balance to remain similar based on our discussion with the agency. Therefore, we will focus our control understanding and testing on the local sales and use tax portion of the balance.

### **(3) Updates to Significant Account Matrix:**

No updates to the Significant Account Matrix is needed.

### **H.2.PRG - Payments of Taxes to Other Governments**

*Procedure Step:* Controls - ATLAS

*Prepared By:* CJM, 10/8/2024

*Reviewed By:* SHW, 10/9/2024

Purpose/Conclusion:

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

#### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.

In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

Who or what initiates the control  
When (or how often) is the control applied  
Who performs the control



## State of Washington

As needed, the experience, knowledge and attitude of the person applying the control

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any exceptions or alternative processing to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

## Financial Statement Audits Planning Guide

Record of Work Done:

### **Material Balance(s) and Assertions**

Internal controls in the Automated Tax and Licensing Administration System (ATLAS) address the following balance(s):

#### **Payments of Taxes to Other Governments - Custodial Fund**

For the following assertions:

**Classification** - There is a risk that local tax payments to other governments were actually state taxes.

**Valuation** - There is a risk that tax payments were incorrectly valued (wrong tax rate).

**Completeness** - There is a risk that not all taxes collected on behalf of local governments have been identified and distributed to those government

### **Gain an Understanding of Internal Controls**

We met with Jason Hartwell, Tax Administration Manager, and Courtney Tornquist, Systems Specialist, on May 8, 2024 to discuss controls related to the Payments of Taxes to Other Governments.

#### Local Tax Rates

Counties, cities, and local tax codes have the authority to assess local taxes in addition to the state's regular 6.5% sales and use tax (use tax is the same rate as sales tax, taxpayers would pay this when purchasing a television in Oregon for example). These taxes are regulated by ordinances or resolutions set by the local governments. Each jurisdiction has a collection agreement on file with DOR that includes the administration fee charged (if applicable) and how refunds and redistributions are handled. When a jurisdiction passes a resolution or ordinance to collect a new tax, they must provide DOR with written notification, a copy of certified election results and a copy of the ordinance or resolution. The jurisdiction must provide the documentation at least 75 days before the effective date (January 1, April 1, and July 1). Taxpayer Account Administration (TAA) has an Excise Tax Examiner (ETE) on the local tax team that will monitor and review election result documentation quarterly to verify if any new taxes or rates have passed.

#### Local Tax (LT) Rate Testing in ATLAS

The process for updating the local tax rates is:

1. A LT manager receives documentation from a jurisdiction indicating they have passed a resolution/ordinance. Once the documents are

## State of Washington

reviewed/verified, the manager puts the changes on a spreadsheet and emails that spreadsheet to the LT system specialist.

2. In a test environment, a programmer updates rate tables as necessary. This environment is verified by reviewing the rates in the Automated Tax and Licensing Administration System (ATLAS) and from various ad hoc reports. Then the changes are moved to the production environment.

3. A programmer will then make system application changes in the test environments. The LT system specialist file test batches (tax returns) for this environment and ensures that they post and calculate properly. ATLAS is then verified for proper accumulation and distribution. Then the application changes are moved to the production environment.

The LT system specialist conducts testing in production to ensure accumulation and distribution amounts are accurate and only local tax codes are included prior to distribution to jurisdictions. TAA will also verify local tax calculations using the new rates on a monthly basis. Money is not distributed to local governments by OST until TAA verifies the data in ATLAS (**Key Control 1 - Valuation/Classification - Manual**). Distributions usually occur the following month after tax returns are due. This allows TAA to work through any identified issues.

### Calculation of Local Sales and Use Tax

Businesses are assigned a location code in ATLAS. The location codes feed back to the jurisdiction for tax collection and local taxes accumulate to the reported locations based on the taxes imposed in each jurisdiction. Filers are required to submit Excise Tax returns where local tax data is captured in ATLAS. The Combined Excise Tax Return form requires businesses input a location name and location code when reporting local sales tax collected. Based on the information input by the taxpayer, ATLAS captures the total taxes collected and sums it up by the type of local tax by location code (**Key Control 2 - Valuation - Automated**). Local sales and use tax are calculated and recorded within ATLAS similar to the other types of tax revenues reviewed at [Retail Sales and Use and B&O Taxes]. If a return is filed with a wrong location code or any errors, the return will error out in the system and will not be recorded until it is manually reviewed and resolved by a TAA examiner. The error will go into a work queue task that is pulled and reviewed by the examiners. If corrections are required, they will make the adjustment and save it in the system.

Local Sales and Use Tax are not the State's and are only collected and distributed by DOR on behalf of the local jurisdictions. When a taxpayer submits a payment, DOR initially uses ATLAS to record the amount in the Suspense Account within the Office of the State Treasurer (OST). The money is held in trust and redistributed monthly by OST. When the payment is applied to the tax return, ATLAS generates a JV to record a "Due to Other Funds" (Short-Term) in AFRS. On the last day of the month DOR enters a JV to reclassify the amount to be distributed by OST as "Due to Other Governments" (MC).

### **How Transactions are Recorded in AFRS:**

#### Gross Receipts Accrual

For monthly filers, Excise Tax returns for June activity are due July 25th. For quarterly filers the tax returns for the 4th fiscal quarter (April, May, and June) are due July 31st. At June 30th, tax has been collected by businesses (taxpayers), from their customers, for sales occurring during the month of June; however, they are not required to file their tax returns and turn over the amount collected on their June sales until July 25th,

## State of Washington

when the June tax return is due. The Due to Other Governments portion is the amount collected by the tax payer for their location (i.e. city) and then sent to DOR when the taxpayer files and remits their monthly taxes (state and local). After year end, an AFRS entry is made to recognize these revenues and due to other governments in the proper accounting period (current year under audit). This is because at June 30th these revenues will not have been recorded (as received or as a receivable) due to Excise Tax returns not being received by year-end.

In August, B&FS runs a report (B9901FI1Y Gross Receipts Accrual Report) in ATLAS to pull data of June excise tax returns and the 4th fiscal quarter (April, May, and June) returns received from July 1st to August 15th. The Department estimates that 90 to 96% of the June returns and the 4th fiscal quarter (April, May, and June) returns are received by the time the report is run and therefore included on the report. Using this report, an AFRS entry is made to show the June returns received as a June 30th receivable and accrued revenue. The accrued revenue is an estimated amount of tax returns that will be paid within 12 months of the fiscal year end.

### Adjusting Entries

We met with Ayano Faasumalie, Revenue and Financial Reporting Coordinator, on May 14, 2024 to discuss the process for recording all tax collections and distributions for FY2024. Due to guidance received from OFM, DOR changed their reporting of local sales and use tax starting in FY21. This change resulted in all collections and distributions of taxes being recorded as additions and deductions in the Fiduciary Statement of Net Position. ATLAS already prepares monthly journal entries to record excise tax receivable, accrued revenue, and unavailable revenue. After ATLAS creates JVs, B&FS has 6 business days to review the JVs before it is transmitted to AFRS. The receivable and revenue calculations are then reversed out for the beginning of the next month. At the end of each month, Revenue Accounting will also prepare a monthly JV to record the distributions of taxes. Revenue Accounting will retrieve a report from the Treasury Management System (TM\$) that shows how much OST distributed to local jurisdictions. Based on this report, a JV is recorded in ATLAS to match the distribution from TM\$. If the JV does not match with the OST reports, the transaction will show up on DOR's unbalanced in-process report.

Using the monthly JVs created by Revenue Accounting and the ATLAS automated JVs, the Revenue and Financial Reporting Coordinator prepares an adjusting entry to record all collections and distributions for each quarter. The Revenue and Financial Reporting Coordinator runs a Webi report for all data included in GL 5152 (Due To Other Governments) for the quarter to determine the amounts to be reported as collections (GL 3205) and distributions (GL 6505). She separates the Webi query into different excel tabs based on funds. For each fund and subsidiary account, she further separates the amounts into the following:

- Collection for Distribution

  - From the prior quarter to be distributed in the current

  - From the current quarter to be distributed in the current

- Distributions

- Collection for Future Distribution

The amounts are summarized in the quarterly Activities Summary by Fund spreadsheet and highlighted to track exactly where the figures came from. Based on the summary, the Revenue and Financial Reporting Coordinator prepares the journal voucher to record collections and

## State of Washington

distributions. The final JV is reviewed and approved by an Accounting Manager, to ensure all collections and distributions are recorded for the quarter (**Key Control 3 - Completeness - Manual**).

### Key controls are as follows:

**Key Control 1 - Valuation/Classification - Manual** - The Local Tax System Specialist conducts testing in production to ensure accumulation and distribution amounts are accurate and only local tax codes are included prior to distribution to jurisdictions.

Taxpayer Account Administration (TAA) will also verify local tax calculations using the new rates on a monthly basis.

**Key Control 2 - Valuation - Automated Calculation** - Based on the location code entered by the tax filer, ATLAS calculates the local sales and use taxes due.

**Key Control 3 - Completeness - Manual** - The Revenue and Financial Reporting Coordinator prepares an adjusting entry to record all collections and distributions for each quarter. The final JV is reviewed and approved by the Accounting Manager to ensure all collections and distributions are recorded for the year and match.

### Noted Weaknesses are as Follows:

None.

### H.2.PR.G - Payments of Taxes to Other Governments

*Procedure Step:* Key Control 1 (Manual)

*Prepared By:* CJM, 6/4/2024

*Reviewed By:* RKM, 6/11/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To confirm whether Taxpayer Account Administration verifies accumulation data in ATLAS prior to distribution to local governments (Key Control 1 for ATLAS) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## State of Washington

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control 1 Valuation/Classification - Manual** - The Local Tax System Specialist conducts testing in production to ensure accumulation and distribution amounts are accurate and only local tax codes are included prior to distribution to jurisdictions. Taxpayer Account Administration (TAA) will also verify local tax calculations using the new rates on a monthly basis.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

On May 8th, 2024, we spoke with Jason Hartwell, Tax Administration Manager for Local Tax, and Courtney Tornquist, System Specialist, about reconciliations performed on a monthly basis to ensure local tax accumulated per jurisdiction are accurate. Courtney performs the quarterly tax rate change testing as well as the monthly production testing. Courtney stated the monthly production testing is done on a sample basis to verify the accumulations are accurate before OST distributes the funds back to the local jurisdictions. During the monthly testing, she will also include jurisdictions that had recent changes. During the meeting they provided a walkthrough of the March 2024 production testing. The March testing included the following jurisdictions:

- 4 - Chelan
- 9 - Douglas
- 28 - San Juan

Each county selected for testing has its own individual tab and data feeds into the summary table where recalculations are compared to accumulation amounts from ATLAS. Any variances not attributed to rounding are investigated and corrected if needed. We noted the system specialist identified a few variances between ATLAS and the recalculated accumulation. The largest variances were reconciled and were identified as variances due to the payment timing of rural state shared tax. We noted the variances were reduced to reasonable differences (no more than 0.5% of variance for any jurisdiction). ***No issues noted.***

### **Noted Weaknesses are as follows:**

None



# State of Washington

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **H.2.PRg - Payments of Taxes to Other Governments**

*Procedure Step:* Key Control 2 (Automated)

*Prepared By:* CJM, 9/30/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion:

### **Purpose:**

To determine whether ATLAS calculates the local sales and use taxes due based on the location code entered by the tax filer (Key Control 2 for ATLAS) was in place in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [Controls - ATLAS].

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

# State of Washington

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

## State of Washington

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and*

# State of Washington

*transaction processing controls.*

## Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

## Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

## State of Washington

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

# State of Washington

## Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

## Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

# State of Washington

## Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

## Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

## Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

## State of Washington

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables*



## State of Washington

*or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

## State of Washington

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

## State of Washington

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3

# State of Washington

is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

## Software Calculation:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## Automated Interfaces:

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

## State of Washington

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Information Technology](#) Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

#### Manual vs. Automated Interfaces

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the*

# State of Washington

*following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process



## State of Washington

to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm

# State of Washington

with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards AU-C 315 Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards AU-C 330 Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control 2 Valuation - Automated** - Based on the location code entered by the tax filer, ATLAS calculates the local sales and use taxes due.

## **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the "Controls - ATLAS" step.

## **STEP 2: Confirm and Test Automated Key Control:**

We obtained tax return information from ATLAS for a sample of taxpayers that paid local sales and use taxes during FY24 and re-performed the tax calculations. See testing at [[Local Tax Collection Distribution Testing - CONFIDENTIAL](#)]

## **STEP 3: Understand General IT Controls**

On May 8, 2024, we met with Jason Hartwell, Tax Administration Manager, and Courtney Tornquist, IT Business Analyst, to gain an understanding of the general IT controls for ATLAS. Maintaining and updating the Department of Revenue's (DOR) Automated Tax and Licensing Administration System (ATLAS) is a large undertaking that requires coordination across multiple areas of the agency. Various division staff routinely prepare change requests (known as SQRs) to correct defects, update, or create new system functionality and configuration. SQRs are the mechanism used to facilitate the process and ultimately become the system of record for the development activities. SQRs must be reviewed and approved via a workflow process within the Fast Code Repository (FCR) environment before its implemented into ATLAS (**General IT Control 1**). Formulas and calculating factors are stored in ATLAS within a programming table and require a SQR to update an automated calculation. The calculations are triggered by the Tax Filer when they submit a tax return. When errors occur during the SQR process an alert will show in the workflow process and a developer will be assigned to correct the error.

# State of Washington

## **SQR Workflow Process**

On May 23, 2024, we met with Lucas Kenall, ATLAS Development & Technology Services Manager. When a change to tax rates are needed a SQR submitter creates a request. A Change Manager reviews the request to ensure it is necessary and filled out correctly. When the request is approved a developer is assigned. The requested changes are made in a testing environment to ensure they are implemented correctly without affecting the active ATLAS rates. When the testing is complete the SQR is placed into staging where it is reviewed to ensure it will function correctly. Approvals from 2 members ATLAS development and Technology Services Team are needed to complete the process. When the staging is complete the SQR is passed to the migration step where it will be automatically deployed to ATLAS during non-business hours. Weekly the ATLAS services team ensures that migrations complete with the proper approvals by running a Migration Audit Report that show all migration statuses and approvals. Once the migration has completed successfully the SQR is closed.

## **STEP 4: Confirm Key General IT Controls**

**General IT Control 1:** SQRs must be reviewed and approved via a workflow process within the Fast Code Repository (FCR) environment before its implemented into ATLAS.

On May 8, 2024, Courtney Tornquist, System Specialist, provided us with screenshots of SQR 15578: Local Tax-Quarter 1 2024 changes. We reviewed the SQR workflow to ensure that each step in the process was signed off and approved before moving on to the required next step. The SQR was initiated by Jason Hartwell on October 18, 2023. The SQR was assigned to Courtney Tornquist. We reviewed the workflow logs for the SQR and noted that each step had notes and approvals showing adequate review. The SQR process was closed on March 12, 2024. **No issues noted.**

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **H.2.PRG - Payments of Taxes to Other Governments**

*Procedure Step:* Key Control 3 (Manual)

*Prepared By:* CJM, 6/4/2024

*Reviewed By:* RKM, 6/11/2024

Purpose/Conclusion:
---------------------

**Purpose:**

## State of Washington

To confirm an adjusting entry to record all collections and distributions for each quarter is prepared (Key Control 3 for ATLAS) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision,

## State of Washington

the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially

## State of Washington

be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 3 Completeness - Manual** - The Revenue and Financial Reporting Coordinator prepares an adjusting entry to record all collections and distributions for each quarter. The final JV is reviewed and approved by the Accounting Manager to ensure all collections and distributions are recorded for the year and match.

The understanding for this system is documented above in the "Controls - ATLAS" step.

### **1. Confirmation of Key Manual Control:**

#### **Quarterly Adjusting Entry Review**

We obtained AFRS journal voucher number 14030250. We noted the explanation of the entry was "To record additions and deductions for Fund 01T, 034, 16C, 17A, 768, 797 for Qtr 1, FY 2024 (July - September, 2023)". Per the line item lead sheet, we noted the majority of the balance is included in fund 034, Local Sales and Use Tax, which is where we focused our control review and testing. We noted the total amount of local sales and use tax collected account was \$1,979,599,134. The collection amounts are based on the monthly JV entries automatically created by ATLAS. We agreed the amounts reported in the JV to a summary of all monthly JVs in quarter 1 from ATLAS. The total collection of local sales and use tax that was distributed in 2024 totaled to \$1,979,599,134. Amounts tie without exception. The JV was prepared by Ayano Faasumalie, Revenue and Financial Reporting Coordinator, on October 23, 2023 and reviewed by Binh Vu, Accounting Manager, on October 23, 2023. ***No issues noted.***

#### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

# State of Washington

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX-** We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW – Test of Key Manual Control:**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at maximum.

### **H.2.PRG - Payments of Taxes to Other Governments**

*Procedure Step:* Risk Assessment

*Prepared By:* CJM, 7/25/2024

*Reviewed By:* RKM, 8/9/2024

Purpose/Conclusion:

#### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

#### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your*

# State of Washington

*basis for this assessment:*

## *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

## *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

## *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

## *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

## *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*



## State of Washington

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Financial Statement Audits](#) Planning Guide

Record of Work Done:

#### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

**Classification - Moderate**

**Completeness - Moderate**

**Valuation - Moderate**

#### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

##### **Automated Tax and Licensing Administration System (ATLAS) -**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

#### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**Classification - Mod**

**Completeness - Mod**

**Valuation - Mod**

#### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement.

**Classification** - We will review a sample of registered taxpayers and ensure tax types are properly categorized as Local Sales and Use Taxes. We will review quarterly JVs to ensure amounts reported as collections/distributions for other governments are only local taxes.

## State of Washington

**Completeness** - We will use the same sample of registered taxpayers as above, review ATLAS for a filed return, and trace revenue to the accumulation GL within ATLAS and to AFRS. We will also review quarterly JVs to ensure monthly automated accumulations within ATLAS were included in the JV and we will review quarterly collection/distribution JVs to ensure that collections and distributions match and are recorded at accurate values.

**Valuation** - We will recalculate taxes paid for the same sample of registered taxpayers as above, to ensure taxes are recorded at proper values and are based on local tax rates and not state tax rates.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### H.2.PRG - Payments of Taxes to Other Governments

*Procedure Step:* Substantive Test

*Prepared By:* CJM, 10/18/2024

*Reviewed By:* RKM, 10/22/2024

Purpose/Conclusion:

**Purpose:**

To determine whether financial statements properly classify local tax collections (Classification).

To determine whether all local tax collections relating to the period were reported (Completeness).

To determine whether local tax collections were reported at properly valued or calculated amounts (Valuation),

**Conclusion:**

We determined:

Financial statements properly classify local tax collections (Classification).

All local tax collections relating to the period were reported (Completeness).

Local tax collections were reported at properly valued or calculated amounts (Valuation).

Testing Strategy:

The following is a list of **considerations** for testing the classification assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

# State of Washington

## **Classification between Line items**

Scan revenue streams or types to evaluate whether they appear reasonable in relation to the line item description. Follow-up on any unexpected results with accounting research to determine correct classification.

Select or sample revenues from high risk populations and review supporting documentation that demonstrates correct classification of revenues.

Search for manual journal entries that re-classify existing revenue balances (transaction is a debit and credit to different revenue accounts). Consider testing if any risk indicators are noted.

## **Classification between Opinion Units**

Search for manual journal entries that transfer revenues from one opinion unit to another without recording a balance sheet transaction, other than a direct charge to fund balance (debit and credit to revenue and fund balance for each opinion unit, respectively). Consider testing if any risk indicators are noted.

Scan revenue streams or types by fund and evaluate whether revenue streams or types appear reasonable in relation to the activities of the fund. Follow-up on any unexpected results with accounting research to determine correct classification.

## **Property Taxes** - see separate step

The following is a list of **considerations** for testing the completeness assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Identify expected revenue streams based on understanding of fund activities and scan to see if revenue is reported for all such streams.

Follow up on any unexpectedly missing streams.

Identify new revenues (ex: new grants or programs) and follow up to verify that expected revenues have been reported.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Trace selected or sampled revenues from source documents to accounting records.

*Source documents may consist of billing, fine, or fee records. Or it may consist of service records that imply a billing, such as license or permit issuance.*

# State of Washington

Perform a multi-year trend of revenues and follow up on unexpected decreases.

Search for manual journal entries that debit (decrease) revenues. Consider testing if any risk indicators are noted.

## **Cut-Off**

Test transactions recorded in the next period to determine whether the revenue should have been recorded in the current period.

*Transactions recorded at the beginning of the next period would generally be considered at highest risk of being improperly shifted to that future period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields. If the population is large, consider stratifying to either scan and select or test 100% of all large value transactions combined with a lower assurance sample for small dollar transactions.*

## **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Calculation**

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

## **Realizable Value**

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

## State of Washington

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### Estimation / Recognition

Review calculation and support for assumptions of any estimated revenues.

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

**Property Tax Revenues** - see separate step

Guidance/Criteria:

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [1.5](#) Determining Operating/Nonoperating/Revenues/Expenses in Proprietary Funds**

**BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

**BARS [3.6.11](#) Suspense Funds**

**BARS [3.6.13](#) Utility Tax (*applies only to cities*)** - should be accounted for as a revenue in the general fund (3164000) and expenditure in the utility fund (53P0040), if the utility passes the tax on to its customers then the additional charges should be recognized as revenue (343P000) directly in the utility fund not in the general fund

Record of Work Done:

### **Tax Collections for Other Governments Testing Coverage**

We reviewed the line item leadsheet [[Line Item Lead Sheet](#)] and noted Fund 034 - Local Sales & Use Tax accounts for the majority all payments of taxes to other governments. We determined focusing our testing on Fund 034 collections would provide sufficient coverage over the balance to meet the relevant assertions. *We performed testing of the local tax collections/distributions simultaneously at the H.1 folder.* See testing details below.

**Substantive tests performed to meet the Completeness assertion:**

## State of Washington

We obtained a list of all active taxpayers that paid local sales and use taxes as of 6/30/2024 and randomly selected a sample of 30 taxpayers for various periods to ensure the return was accurately filed and posted to AFRS. Jason Hartwell, Tax Administration Manager, provided a screenshot of all selected taxpayers' tax returns entered in ATLAS as well as their payment of the calculated taxes. We reviewed the return for the selected taxpayers in ATLAS to ensure a return was filed and payments were received for the entire amount recorded in the return. See testing performed at [Local Tax Collection Distribution Testing - CONFIDENTIAL]. **No issues noted.**

Business and Financial Services makes an adjusting entry to record local tax collections as tax collections for other governments and tax payments to other governments to comply with GASB 84 regulations on a quarterly basis. When payments for local taxes are collected, ATLAS automatically accumulates revenues to the appropriate fund and GL in a monthly JV. The quarterly collection/distribution JVs includes the monthly accumulation JV activity and moves 5152 - Due to Other Governments to the revenues and expenditures GL (32XX and 65XX). We reviewed each quarter's adjusting JV to ensure:

- All automated ATLAS JVs are recorded and in the proper period
- Quarterly JV amounts only include local taxes
- Collections and Distributions for each month match

We noted the quarterly JVs were complete based on the testing above. See testing at [Quarterly Collection Distribution JVs]. **No issues noted.**

### **Substantive tests performed to meet the Valuation assertion:**

Using the same randomly selected sample of 30 taxpayers, as mentioned above, we recalculated taxes paid based on local tax rates to ensure that revenues related to local sales and use tax were valued at proper amounts and based on local tax rates and were not related to state tax revenues. Jason Hartwell, Tax Administration Manager, provided a screenshot of all selected taxpayers' tax returns entered in ATLAS. We obtained the local sales and use tax rates for each selected period from the DOR website. Based on the taxable amount in the tax returns, we recalculated the collected local sales and use tax. Any differences noted were small rounding errors. We determined all selected local sales and use tax collections/distributions were reported at properly valued and calculated amounts. See testing performed at [Local Tax Collection Distribution Testing - CONFIDENTIAL]. **No issues noted.**

### **Substantive tests performed to meet the Classification assertion:**

Using the same randomly selected sample of 30 taxpayers, as mentioned above, we tested to ensure that collections/distributions were properly categorized as Local Sales and Use Taxes. Jason Hartwell, Tax Administration Manager, provided a screenshot of all selected taxpayers' tax returns entered in ATLAS. We obtained the local sales and use tax rates for each selected period from the DOR website. We reviewed the ATLAS tax returns to ensure that only local agencies were included and selections were properly categorized as local city or county taxes collected as use, sales tax, or deferred sales tax. We determined all selected taxpayers were properly categorized and reported. See testing performed at [Local Tax Collection Distribution Testing - CONFIDENTIAL]. **No issues noted.**

Business and Financial Services makes an adjusting entry to record local tax collections as tax collections for other governments and tax payments

## State of Washington

to other governments to comply with GASB 84 regulations on a quarterly basis. When payments for local taxes are collected, ATLAS automatically accumulates revenues to the appropriate fund and GL in a monthly JV. The quarterly collection/distribution JVs includes the monthly accumulation JV activity and moves 5152 - Due to Other Governments to the revenues and expenditures GL (32XX and 65XX). We reviewed each quarter's adjusting JV to ensure:

Quarterly JV amounts only include local taxes

We noted the quarterly JVs were classified appropriately based on the testing above. See testing at [[Quarterly Collection Distribution JVs](#)]. ***No issues noted.***

### H.3.PRG - Cash & Cash Equivalents

*Procedure Step:* Summary & Conclusion

*Prepared By:* DRR, 12/9/2024

*Reviewed By:* RKM, 12/9/2024

Purpose/Conclusion.:

#### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

#### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy.:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider



## State of Washington

the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the [Permanent File](#) by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

Is information precise enough to catch if misstatements exceeded the tolerable level?

Is information detailed enough to conclude on whether or not there were misstatements?

Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?

How did misstatements occur and how often might they occur again in the population?

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

## State of Washington

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the **FS Summary & Report** step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the **Material Balances** spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

### **H.3.PRG - Cash & Cash Equivalents**

*Procedure Step:* Understanding of Line Item

*Prepared By:* DRR, 12/6/2024

*Reviewed By:* RKM, 12/9/2024

# State of Washington

Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

We determined the large increase in GL 1110 Fund 148 was due to an error by the College. **See issue [V: WSU\_Cash and Accrued Liabilities (Part of ML)]. See AOM [Aggregation of Misstatements (GAAP)].**

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

## State of Washington

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions:**

We reviewed the prior audit and did not note any exceptions relevant to these line items.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

We met with Angela Marie Dobbins, Executive Director, and Tami Bidle, Associate Controller on November 21, 2024 to gain an understanding of the Cash & Cash Equivalents balance. Per Tami, the majority of this balance is comprised of two bank accounts, both held at Bank of America and the LGIP Accounts. The bank accounts are the Non-Federal Account and the Student Loan Account.

When reviewing the leadsheet and the ACFR data for the college, we noted that the overall balance balance increased approximately \$188.7 million over the prior year. This was primarily due to an increase in GL 1110 "Cash in Bank" for fund 148 of \$311 million. This large increase was

## State of Washington

due to an error the College identified after we requested bank statements and bank reconciliations to test the balance. **See issue and AOM links in conclusion.**

Additionally, we noted there were several large decreases in GL 1205 "Temporary/Pooled Cash Investments" for funds 148, 149 and 846 totalling approximately \$94.2 million. Lastly, there was a significant decrease in GL 5155 "Due to Other Funds - Pooled Cash & Investments" for fund 148 of \$95.9 million.

### **(3) Updates to Significant Account Matrix:**

We identified no changes that need to be made to the Significant Account Matrix.

### **H.3.PR.G - Cash & Cash Equivalents**

*Procedure Step:* Controls - Cash Reconciliations

*Prepared By:* DRR, 11/26/2024

*Reviewed By:* RKM, 12/9/2024

Purpose/Conclusion.\*

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done. We noted that the College did not perform a thorough review to ensure all entries were recorded in the State's accounting system. **See issue [V: WSU Cash and Accrued Liabilities (Part of ML)].**

Testing Strategy.\*

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.

In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

Who or what initiates the control

When (or how often) is the control applied

Who performs the control

## State of Washington

As needed, the experience, knowledge and attitude of the person applying the control

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any exceptions or alternative processing to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Financial Statement Audits](#) Planning Guide

Record of Work Done:

Internal controls in Cash Reconciliations address the following balance(s):

Cash & Cash Equivalents

For the following assertions:

Existence - There is risk that reported cash and cash equivalents don't match reconciled bank accounts and records.

#### **Gain an Understanding of Internal Controls**

We met with Angela Marie Dobbins, Executive Director, and Tami Bidle, Associate Controller on November 21, 2024 to gain an understanding of the cash reconciliation process. We also met with Arthur Whitten, Director of Treasury Services, and Jill Renna, Senior Treasury Analyst on November 26, 2024 to gain an understanding of the Local Government Investment Pool (LGIP) investment process.

Washington State University has approximately 30 bank accounts, however, most of these accounts do not roll up into FBG - Higher Education Special Revenue. Workday requires that each fund has a bank account attached and this is how the College is able to determine which fund is associated with the accounts and allows the College to determine how to upload the cash data into AFRS and which amount will be rolled up into special revenue rollup fund FBG.

#### **Cash Reconciliation**

After month end, the Bank Team staff will obtain the bank statements for their accounts, and run multiple Workday reports for each of these accounts. The two most important Workday reports for the reconciliations are the Outstanding Payments, and In-Transit reports, which will provide the Bank Team with lists of all the reconciling items they will use to reconcile the bank accounts. The reconciliations will typically be performed by Gail Nash, Fiscal Manager, and she will send them to Tami Bidle, Associate Controller, who will review the reconciliation to ensure that there aren't any transactions missing from the reconciliation and that the cash reported in Workday exists (**Key Control #1 - Existence**).

#### **Investments**

Washington State University has 3 LGIP accounts - one operating account, one for major gifts (Engineering Building Construction), and one for the student corporation. We will document the process for the operating account - Fund 148, as this is the main account that rolls up into FBG - Higher Education Special Revenue, but the process is similar for all of the LGIP accounts.

Arthur Whitten, Director of Treasury Services, and Matt Skinner, Deputy Chief Financial Officer, are the only WSU employees who can make LGIP



## State of Washington

transactions. On a daily basis, Jill Renna, Senior Treasury Analyst, will log the daily withdrawal and deposit transactions for the LGIP into Workday. At month end, Jill will use Secure Access Washington (SAW) to download the LGIP statements, and run a report of the LGIP balances in Workday to ensure that all of the transactions are recorded in Workday. To record monthly earnings on investments and the reinvestment of these earnings into Workday, Arthur will typically create the journal entry and the Vice President of Finance will review the JE to ensure that investment earnings existed at period end **(Key Control #2 - Existence)**.

Once these tie outs have been completed, Arthur will let Tami Bidle, Associate Controller, know that the investment balance is ready for upload to AFRS, and she will perform the last verification before uploading the Workday balances into AFRS in their monthly upload.

### **How Transactions are Recorded in AFRS:**

Once a month, WSU's Banking Team will close their books, and upload their Workday data into AFRS.

### **Key Controls are as Follows:**

**Key Control #1** - The Associate Controller will review reconciliations and reconciling items to ensure reported cash existed at period end **(Existence)**.

**Key Control #2** - Journal Entries are created and reviewed to ensure that investment earnings are recorded and existed at period end **(Existence)**.

### **Noted Weaknesses are as Follows:**

The University did not perform a thorough review to ensure all entries were recorded in the State's accounting system. **See issue in conclusion.**

### **H.3.PRG - Cash & Cash Equivalents**

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* DRR, 11/26/2024

*Reviewed By:* RKM, 12/7/2024

Purpose/Conclusion.
---------------------

### **Purpose:**

To confirm cash reconciliations were reviewed by the Associate Controller **(Key Control 1 - Cash Reconciliations)** in order to assess control risk.

# State of Washington

## **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls. However, we did note that the College does not document the bank reconciliation review. **See issue** [E: WSU Bank Reconciliation Review Documentation].

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent

## State of Washington

material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. *Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. *Controls are not related to a "significant risk" identified in the audit plan.*

## State of Washington

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Cash and Cash Equivalents - Existence**

**Key Control 1 (Existence - Manual):** The Associate Controller will review reconciliations and reconciling items to ensure reported cash existed at period end (**Existence**).

The understanding for this system is documented above in the "Controls - Cash Reconciliations" step.

### **STEP 1: Confirm Key Controls**

Angie Dobbins, Executive Director/Controller, screenshared Washington State University's June 2024 bank reconciliation for the Non-Federal Local Funds Account ending in 4972. We noted that the banks adjusted ending balance was \$6,143,897.95 and the General Ledger balance was \$6,148,017.69 for a difference of \$4,119.74. We can see that the control is in place and that the College is performing reconciliations, but there was no documentation that the review is taking place. As such, we have made a recommendation for the College to document who performed the reconciliation, who reviewed/approved the reconciliation and the dates on their documents. **See issue in conclusion.**

### **STEP 2: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 3: Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

# State of Washington

## H.3.PRG - Cash & Cash Equivalents

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* DRR, 11/26/2024

*Reviewed By:* RKM, 12/7/2024

### Purpose/Conclusion:

#### **Purpose:**

To confirm investment earning journal entries were reviewed by the Vice President of Finance (**Key Control 2 - Cash Reconciliations**) in order to assess control risk.

#### **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has*

## State of Washington

*been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional*

## State of Washington

*testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Cash and Cash Equivalents - Existence**

**Key Control 2 (Existence - Manual):** Journal Entries are created and reviewed to ensure that investment earnings are recorded and existed at period end (**Existence**).

The understanding for this system is documented above in the "Controls - Cash Reconciliations" step.

# State of Washington

## **STEP 1: Confirm Key Controls**

Arthur Whitten, Director of Treasury Services, shared his screen via Teams on November 26, 2024 to show their fiscal year end journal entry # JE0000274205 to record LGIP investment earnings. We noted that the total debits/credits for the JE were \$2,646,103.02. The JE was created by Arthur on July 1, 2024 and was approved by Arthur's supervisor Matt Skinner, Vice President of Finance on July 2, 2024. **No issues noted.**

## **STEP 2: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **STEP 3: Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **H.3.PR.G - Cash & Cash Equivalents**

*Procedure Step:* Risk Assessment

*Prepared By:* DRR, 11/25/2024

*Reviewed By:* RKM, 12/7/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

## **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.



## State of Washington

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

## State of Washington

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria.†

### **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done.
----------------------

**(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Existence – HIGH

**(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

Cash Reconciliation – **MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

**(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Existence – HIGH

**(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

We will test fiscal year end cash and cash equivalent balances to ensure that cash and cash equivalent existed at fiscal year end.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

**H.3.PR.G - Cash & Cash Equivalents**

# State of Washington

*Procedure Step:* Substantive Test  
*Prepared By:* DRR, 12/9/2024  
*Reviewed By:* RKM, 12/9/2024

## Purpose/Conclusion:

### **Purpose:**

To determine whether reported cash and cash equivalents existed as of the end of the period (**Existence**).

### **Conclusion:**

We determined that reported cash equivalents existed as of the end of the period, and we determined that **reported cash did not exist** as of the end of the period. **See issue here** [V: WSU Cash and Accrued Liabilities (Part of ML)].

## Testing Strategy:

### **SAO Policy Requirement: Confirming or Verifying Cash & Investment Balances**

Confirmations can either be blind or a positive confirmation. In a blind confirmation (sweep), the auditor requests information on all accounts the bank holds for the entity (by entity name and/or EIN). In a positive confirmation, the auditor lists accounts (or accounts and balances) per the entity and asks the bank to confirm that the information is correct.

Confirm cash and investment account balances with County Treasurer, bank and/or brokerage. Use the template confirmation form provided in the Store when needed.

Confirmations can be mailed to addresses listed on the Bank Confirmation Address List available on the Auditor Reference Guide. If the bank notifies you of a different address, please contact Team Audit Support to update the list.

Banks may confirm incorrect amounts either due to a simple mistake, use of a wrong confirmation date or incorrectly including or excluding accounts. The first step in resolving differences should be to check information against the entity's bank statements and then call the bank to specifically confirm any difference.

Confirming investments may involve physical inspection, confirmation with the issuer, confirmation with the custodian, confirmation of unsettled transactions with the broker/dealer, confirmation with the counterparty, and/or reading executed partnership or similar agreements. When confirming investments, ensure investments are held in the entity's name.

## State of Washington

*If confirmations are not used*, auditors must at minimum verify balances to the County Treasurer, bank and/or brokerage statements. If this is done, the auditor should consider the risk that the statements were altered and should examine papers for indications of alteration.

The following is a list of **additional considerations** for testing the existence assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Bank Reconciliations**

If the auditor is comparing reconciled (confirmed) bank or county treasurer balances to the GL (rather than confirmed amounts within an expected variance due to reconciling items), the auditor should consider performing some or all of the following tests to verify the accuracy of the reconciliations. Note that testing the reconciliation will provide evidence of both the existence and completeness of cash and investment balances.

Trace (or compare summed) bank balances per statements to reconciliations.

Trace (or compare summed) book balances per reconciliations to the general ledger or financial statements.

*If a cash account is allocable to a particular fund, the balance in the general ledger should be recorded in the same fund.*

Scan the reconciliation for reasonableness. Look for unusual, unexpected or vaguely described reconciling items, lack of support or detail, very large reconciling items, very old reconciling items, and missing or extra elements that would indicate that the reconciliation was being performed incorrectly.

Foot the reconciliation for accuracy.

Trace deposits in transit to the subsequent month's bank statement, considering reasonableness of the in-transit period.

Trace outstanding checks to cash disbursement journal.

Check that any other reconciling items are valid and have been properly accounted for (ex: large debit or credit memos).

Check reconciliation against prior and/or subsequent reconciliations for reasonableness of amounts and items included and to trace reconciling items from the previous and/or subsequent period.

### **Other Tests**

Inquire whether any checks or deposits were being held at year end for budget, cash flow or other purposes.

Confirm investments purchased but not received as of year-end

Confirm investments sold but still held as of year-end

Confirm interest due or accrued but not yet received as of year-end

Search for manual journal entries that debit (increase) cash. Consider testing if risk indicators are noted.

# State of Washington

Review reconciliations of clearing and transmittal accounts.

See accountability steps for testing strategies related to petty cash and imprest funds, which are not expected to be material to the financial statements.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Outstanding Checks and Deposits in Transit** – Per TIS section 1100.08 (AICPA Technical Questions and Answers), outstanding checks should be reported as a reduction of cash and the amount of deposits in transit should be reported as cash. A check is considered outstanding from the time that it is out of the payor's control – when mailed or delivered to the payee – until the time it clears the bank. Cash should represent amounts within the control of the reporting entity, that is, the amount of cash in banks plus cash and checks on hand and deposits in transit minus the amount of outstanding checks.

**SAO Audit Policy [6350](#) – External Confirmations**

**[Investments](#) Area Guide**

**[LGIP Fund Summary Reports](#)** - includes a list of local government accounts and balances in the Local Government Investment Pool

Record of Work Done:

## **Substantive tests performed to meet the Existence / Occurrence assertion:**

We ran a query using the ACFR database to determine which balances were significant for testing. We initially determined that GL 1110 fund 148 and GL 1206 fund 148 were the significant balances for our testing as they provided 81 percent coverage of the Washington State University (WSU) roll up fund FBG cash & cash equivalent balance. We asked Angie Dobbins, Executive Director/Controller, and Tami Bidle, Associate Controller, for the June and July 2024 bank statements and reconciliations related to these AFRS balances.

After our request, Angie mentioned that as they analyzed the cash reported in AFRS GL 1110 for fund 148, the University identified an entry that was not entered into AFRS and would need to be corrected. She mentioned the balance in GL 1110 fund 148 would change from \$311,373,440.20 to approximately \$5,193,359.83. Once we became aware of the issue above, we updated our balances for testing to ensure we obtained sufficient

## State of Washington

coverage of the roll up fund FBG cash and cash equivalent balances for WSU. We modified out testing coverage to approximately 87 percent of the FBG cash and cash equivalent balance for WSU. We determined that this was sufficient coverage of the balance. See "Summary" tab here [[Cash & Cash Equivalent Testing](#)]. **See issue and AOM links in the conclusion above.**

### LGIP Balances

We obtained the June 30, 2024, Local Government Investment Pool (LGIP) statements from Arthur Whitten, Director of Treasury Services. We were able to tie ending account balances directly to our AFRS database query results to ensure the LGIP balances existed without exception. See LGIP testing here [[Cash & Cash Equivalent Testing](#)]. **No issues noted.**

### Temporary / Pooled Cash Investment Balances

We obtained the June 30, 2024, investment statement for account ending 6300, and "Final AFRS Investment Trial Balance 063024.xlsx" from Arthur Whitten, Director of Treasury Services. We used the investment statement to find the ending historical/revalued costs for total assets and cash equivalents, and to manually calculate the total short term investments. We used the trial balance to recalculate the percentage of the investment account balance that would be uploaded to AFRS in each fund using the figures we took from the investment statements. We were able to recalculate the percentage of the investment balance that would be uploaded to AFRS with a variance that was below the floor. See investments testing here [[Cash & Cash Equivalent Testing](#)] **No issues noted.**

### I.1.PRG - Cash & Investments

*Procedure Step:* Summary & Conclusion

*Prepared By:* CJM, 11/20/2024

*Reviewed By:* CJG, 11/21/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

#### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

# State of Washington

## Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

Does evidence relate to the population, period of time and risk (assertion and "what could go wrong" from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

Is information precise enough to catch if misstatements exceeded the tolerable level?

Is information detailed enough to conclude on whether or not there were misstatements?

Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:



## State of Washington

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?

How did misstatements occur and how often might they occur again in the population?

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined the results of substantive tests do not indicate a need to modify our risk assessment (IR, CR and RMM).

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We determined the quality and quantity of evidence obtained was sufficient and appropriate.

# State of Washington

## I.1.PRG - Cash & Investments

*Procedure Step:* Understanding of Line Item

*Prepared By:* SHW, 4/30/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To gain an understanding of cash and investments managed by the State Treasurer's Office.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

## State of Washington

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Prior Audit Exceptions:**

We noted in the prior years audit that interest earned, totaling \$27,141,123, was reported as accrued interest rather than investments by the State Treasurer's Office. We made a verbal recommendation that the Treasurer and OFM include interest earned and received in June as part of cash and investments reported at fiscal year end. We followed up with Denise Nguyen, OST Accounting Services Manager, on April 8, 2024 and found no changes have been made to the Treasurer's accounting policies/procedures to date but they expect to confer with OFM to discuss

# State of Washington

accounting changes prior to FY24 year-end close.

## **(2) Composition & Change Analysis:**

Line Item Lead Sheet: [[Line Item Lead Sheet](#)]

The Office of the State Treasurer's (OST's) responsibilities include managing the cash flow of all major state accounts and allocating cash to investments (both long-term and short-term). Here, we will gain an understanding of the following balances as shown on the lead sheet:

Cash and Cash Equivalents (sort codes 1A and AC)

Restricted Cash and Investments (sort codes 1H and AF)

Investments (sort code AM)

OST's allocation to investments includes the Local Government Investment Pool (LGIP). LGIP investments (sort codes AM, DJ, BE, LF, and TW) are examined by an external CPA audit, and we will place reliance on their work as documented at: [[Work of Other Auditors - LGIP](#)].

For interim planning, we selected the majority of cash and cash equivalents and investment accounts as significant accounts in the significant balance spreadsheet at: [[Interim Planning Significant Balance Spreadsheet](#)]. SAO policy requires that we select all cash balances as material, however, the Higher Education Student Services Fund contains balances that are quantitatively small and spread across multiple Colleges and Universities. Cash and Pooled Investments can be separated into the following treasury type codes for analysis:

T = Treasury

U = Treasury Trust

L = Local (Accounts outside control of OST)

We used the treasury codes referenced above to determine cash coverage for each agency and opinion unit. Only the Treasury (T) and Treasury Trust (U) accounts are under the Treasurer's control. Local accounts (L) are controlled by each agency or department. Therefore, in computing our cash and investment(s) line item audit coverage, we will exclude funds held in local accounts.

## **Restricted Cash and Investments**

Restricted Cash and Investment line item(s) include the following GL account balances: \*Note: GL Codes listed in [SAAM 75.40.20](#)

### **GL 1140 Restricted Cash and Investments - Current Operations**

GL code is used to record restricted cash and investments held by escrow agents and trustees that will be used in current operations for the payment of current liabilities.

Fund Statement Sort Code: GL Sort Code AF, Restricted Cash and Investments (AFRS D54 Table)

Statement of Net Position Sort Code: Gov't Wide Sort Code 1H, Restricted Cash and Investments (AFRS D54 Table)

# State of Washington

## **GL 1240 Restricted Cash and Investments - Noncurrent**

GL code is used to record cash and investments held by escrow agents and trustees that are restricted and will not be used in current operations.  
Fund Statement Sort Code: GL Sort Code AF, Restricted Cash and Investments, DM Restricted Cash and Investments- Non-current (AFRS D54 Table)  
Statement of Net Position Sort Code: Gov't Wide Sort Code 1H, Restricted Cash and Investments, 1S Restricted Cash and Investments - Non-current (AFRS D54 Table)

## **GL 1150 Cash with Fiscal Agents**

GL code is used to record cash deposited with fiscal agents for the payment of state obligations. Amounts held may be restricted.

OFM requires agencies to complete a disclosure form at FYE to identify any balances that may need to be restricted. OFM staff makes a worksheet adjustment to allocate restricted cash and investment balances at the roll-up fund level. This adjustment is not reflected in AFRS but will affect the balances on the financial statements. The current year adjustments will be reviewed as part of our year-end procedures for the FY24 ACFR audit.

## **(3) Updates to Significant Account Matrix:**

We identified no updates to the Significant Account Matrix based on our understanding of the line item.

## **I.1.PRG - Cash & Investments**

*Procedure Step:* Controls - TM\$  
*Prepared By:* SHW, 4/30/2024  
*Reviewed By:* RKM, 8/22/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

# State of Washington

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

## State of Washington

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:
----------------------

Internal controls in the **Treasury Management System (TM\$)** address the following balance(s):

## ***Cash and Cash Equivalents***

- Governmental Activities - GOV - Opinion Unit
- Business-Type Activities - BUS - Opinion Unit
- Fund FAA - General Fund - Opinion Unit
- Fund FBF - Wildlife and Natural Resources - Opinion Unit
- Fund FBG - Higher Education Special Revenue Fund - Opinion Unit
- Fund FEA - Higher Education Endowment - Opinion Unit
- Fund FFJ - Health Insurance - Opinion Unit
- Aggregate Remaining Funds - NON - Opinion Unit

## **For the following assertions:**

- Existence - That cash and cash equivalents are not on hand, in transit, on deposit with third parties (depositories) in the name of the State, or are held by a third party (trust or custodian agent) on behalf of the State.
- Completeness - Accrued investment income may not be recognized and as a result all cash/investments are not reported.

## ***Investments***

- Fund FAA - General Fund - Opinion Unit
- Fund FFH - Higher Education Student Services - Opinion Unit

## **For the following assertions:**

- Existence - That investments are not on hand, in transit, on deposit with third parties (depositories) in the name of the State, or are held by a third party (trust or custodian agent) on behalf of the State.



# State of Washington

Completeness - All investments are not reported.

Classification - Investments may not be classified as to current and long term based on maturity dates and are not reported in the proper fund type

## ***Restricted Cash and Investments***

Governmental Activities - GOV - Opinion Unit

Fund FAA - General Fund - Opinion Unit

Fund FBG - Higher Education Special Revenue Fund - Opinion Unit

Aggregate Remaining Funds - NON- Opinion Unit

## For the following assertion:

Classification - OFM as the financial statement preparer may be unaware of restrictions placed on cash and investments based on information in AFRS.

NOTE: The controls ensuring that cash is properly restricted take place at OFM, not the Office of the State Treasurer (TRE), and will be addressed in the "Controls - Restricted C&I" step.

## **Gain an Understanding of Internal Controls**

### **A. Background**

#### **Funds:**

The Office of the State Treasurer (TRE) invests daily for Fund 076, the State Treasury Income Account for State Agencies and Fund 523, the Public Funds Investment Account, for the Local Government Investment Pool (LGIP). It also invests on an irregular basis for Fund 845, which is a separately managed account (SMA). This account holds longer term securities, so its activities are irregular.

#### **Bank Contracts:**

TRE contracts with two different banks:

The Concentration Account is contracted with US Bank and holds all Treasury and Treasury Trust Funds.

The Custodian Account is contracted with Northern Trust for investment purposes.

TRE uses US Bank to hold the LGIP funds.

An external auditor audits cash held in the LGIP account and we rely on the work of the external auditor.

#### **System:**

TRE uses the Treasury Management System (TM\$) as the primary system to account for the cash investing cycle. It is a subsidiary accounting system that uploads to AFRS at the end of each business day.

# State of Washington

## Key Roles

Three divisions at TRE perform integral parts of the investment process: The Investment Division, the Investment Accounting Division, and the Cash Management Division. The following summarizes their functions:

Investment Division – execute trades throughout the day, enter into TM\$. Initiates the wiring of funds to and from Custodian Account.

Investment Accounting Division – verify trade tickets settled for the day and confirm in TM\$. Following day, reconcile AFRS balances from previous day.

Cash Management Division – moves money by executing daily wires in or out between the concentration (US Bank), LGIP, verifies all wires have completed properly and that accounting documents are entered into TM\$, and backs up the Investment Accounting Division for work on custodian (Northern Trust) accounts.

*See auditor prepared flowchart for high-level overview of daily process at: [OST Flowchart of Key Controls Cash & Inv]*

We gained an understanding of controls at each division, as documented below:

### 1. Investment Division Staff

This division directs the investing of excess cash through sales and purchases of investments. Investment staff determine the investing amounts for fund 076 and 523 on a daily basis, and fund 845 when needed. The investment division initiates and wires funds from the LGIP to local governments when they receive requests for withdrawals from members. LGIP staff also account for all incoming wires from local governments that are deposited in the pool. Employees initiate wires to transfer funds from Northern Trust (custodian bank) to fund(s) 076, 523 and 845. **We verified and updated our understanding with Chris Matoon, Portfolio Administrator, on March 26, 2024.**

### 2. Investment Accounting Division Staff

Staff ensure portfolio transactions are accounted for properly. Accounting staff also ensure that the bank, TM\$, and AFRS reconcile. The Investment Accounting Division cross-trains their staff members so different roles may be performed by multiple staff members. **We verified and updated our understanding with Denise Nguyen, Accounting Services Manager, and Alexis Lopez, Fiscal Analyst Accounting Manager, on April 4, 2024**

### 3. Cash Management Division Staff

By law, this group acts as the bank for most state agencies. Cash management staff perform duties linking the State's bank concentration account and state agencies. A few agencies, like Higher Education and Employment Security Department, operate locally controlled bank accounts outside TRE. Once the Investment Division initiates a wire, Cash Management Staff receive the authority and responsibility to process wire payments, ACH files (between agencies), and receipt investment transaction sales. **We verified and updated our understanding with Vicki Boudia, Banking Services Administrator, on April 2, 2024.**

## B. Control Activities

### Day 1 - Trade Purchases/Sales

# State of Washington

## **Investment Division Process**

Every morning, Shawn Reed, Portfolio Manager, reviews the cash projections to see what will settle that day to determine overnight investment needs. Shawn informed us that she will also check bank balances to review the prior day's activity. Portfolio managers review TM\$ reports to determine investment decisions for longer term portfolios.

## ***Placing Trades***

Investment Division Staff purchase and sell investments throughout the day using the Bloomberg investment platform. Most of these trades settle on the following business day after the actual trade date except for overnight repos (repurchase agreements), which settle on the same day. Chris Mattoon, Portfolio Administrator, uses trade tickets produced in Bloomberg from all investment staff members and enters trades into TM\$. Shawn Reed or Amanda Hudson, Portfolio Manager, perform Chris's duties if he is unavailable. Northern Trust, TRE's custodian bank, determines investment valuation. Investment Division staff receive an electronic feed from Northern Trust of the fair market value amount(s) through TM\$.

Northern Trust constructs its prices from a variety of sources, with the three main sources used being ICE-IDC, Thomson-Reuters, and Bloomberg. Investment professionals consider their main sources as three of the most highly reputable, trusted, and widely used pricing sources for the current investment market. Investment staff determined they can rely on Northern Trust's fair value pricing based on the reputation of their pricing sources and trusts the provided accuracy. Portfolio Managers rely on their experience in trading to determine if Northern Trust provided an unreasonable price. When investment staff determine a price is unreasonable, they run reports in Bloomberg to further evaluate the price. For example, Bloomberg's "B-val" report performs a simulation of a similar security, which is compared to Northern Trust's valuation. TM\$ alerts Investment Division staff when prices change in excess of 10% of their previous value via an email to staff with a report which they use to investigate the price warning. This is extremely rare and has not occurred in FY24 as the Treasurer invests in high quality dollar denominated debt securities with quoted market prices and collateralized mortgage obligations are not allowed.

After trades occur, the Portfolio Administrator manually prepares the daily ticket summary in Excel with all the settling purchases and sales for the day. Once complete, the Portfolio Administrator emails the trade tickets and daily ticket summary to the Investment Accounting Division (**Key Control #1 - Existence, Completeness**). Portfolio Managers email trade tickets for investment transactions that could include purchases and sales of treasury notes, bonds, and discount notes to the Accounting Division email box, who then validate the information entered into TM\$. Once these trades settle, the tickets will be included on a future daily ticket summary. Repurchase agreements, cash deposits, and cash withdrawals settle on the same date as the trade. Investment Division staff email the Investment Accounting Division with all settled transactions for the day along with the daily ticket summary, which ensures timely settlement. This process concludes Day 1 activities and transitions to Day 2, as further described below.

## ***Initiation and Review of Incoming and Outgoing Investment Wires***

The Investment Division initiates all wires between the Custodian account (Northern Trust) and the Concentration account. Each afternoon, the Investment Division accesses a report from Northern Trust (Custodian) showing that all trades have settled and reports the cash balance in each of the accounts. A Portfolio Administrator matches the cash balances to what is displayed in TM\$. If there are no discrepancies, the Administrator

## State of Washington

initiates the wire. To initiate the wire, an Administrator logs into Northern Trust's website using their user name and password as well as a multi-factor authentication security token. After the wire is initiated, a second employee from the Investment Division releases the wire after comparing the wire amounts to the displayed amount in TM\$. Northern Trust's website prevents the same person from initiating and reviewing the wire (**Key Control #2 - Existence**).

### **Investment Accounting Division Process**

As noted above, the Investment Division sends trade tickets for future settlement to the Investment Accounting Division's inbox. Once the Investment Accounting staff receive the new trade tickets in the afternoon, they print out the TM\$ "Trade Verification." A fiscal analyst cross checks the tickets to the TM\$ "Trade Verification" screen printout, ensuring key information such as fund number, transaction type, CUSIP, settlement amount, trade and settlement date(s) par amounts, interest rate, broker name, and security classification all match. Investment Accounting Staff also compare the information in TM\$ on the "Detail Projection Receivable-Cash Receipts" report with the projection report from Northern Trust-"Projected Cash Detail-today" report (**Key Control #3 - Existence, Completeness**). Investment Accounting Staff confirm reports against the cash detail to confirm values are the same and identify any unexpected changes or transactions in advance. The Investment Division and the Investment Accounting division communicate throughout the day to ensure there are no discrepancies or errors known between departments.

### **Day 2 - Final Confirmation and Investment Activities**

#### **Investment Accounting Division Process**

On the day following the trade date, a fiscal analyst repeats procedures from the previous day with updated reports to ensure all information in TM\$ is accurate. Another fiscal analyst then reviews the work at a subtotal level by reviewing the Confirmation screen in TM\$ and the "Projected Cash Detail-Today" from Northern Trust to re-confirm the final transaction amounts. Chris Mattoon, Portfolio Administrator, from the Investment Division, emails the Accounting Services Division with any differences he sees between Northern Trust and TRE. The fiscal analyst also verifies and adjusts interest amounts where rounding is needed. Rounding typically causes differences between Northern Trust's rate calculations and individual line item subtotals. When values differ, TRE uses Northern Trust values as they are the exact amounts received by Northern Trust.

The fiscal analyst prints out the TM\$ Verification Screen and verifies it with the daily trade tickets and other transactions to make sure all the transactions exist and are completely recorded in TM\$. The analyst also ties TM\$ to a "Daily Ticket Summary" report, which is sent to the Investment Accounting Division by the Investment Division Staff when they are done with the morning trading. The "Daily Ticket Summary" also contains information on reverse repurchase, repurchase trades, and CDs. These transactions trade and settle on the same date and do not have activity on day one (see write up above of day one).

For all three funds (076 Concentration Account, 523 LGIP and 845 SMA), if the total amount received from sales, maturity, and interest, is less than the amount needed for planned purchases, the Investment Division wires the difference between US Bank and Northern Trust. If the amount coming in from maturity is more than the amount of scheduled purchases, TRE receives a wire for the difference from Northern Trust to US Bank. Investment Accounting Staff receive another email from Chris Mattoon, Portfolio Administrator, to notify them that the investment activities have

## State of Washington

settled for the day. Investment Accounting then use the Pre-Confirm report and checks it against the TM\$ Confirmation Screen (**Key Control #3 - Existence, Completeness**). This control ensures investment data input is correct, all transactions are recorded in the correct period, transactions actually exist, and TM\$ settle amounts are correct.

To create the accounting transactions & documents in TM\$, Investment Accounting staff click the "confirmation" button and TM\$ automatically sends an email to the Cash Management Division and the Investment Accounting alerting them to the confirmation status.

After the final confirmation in TM\$, the fiscal analyst clicks the reports button to receive emailed reports from TM\$, which are used for reconciliation purposes later on:

- Purchases for Accounting Transactions for Funds 076 and 523 (and fund 845 if applicable)
- Redemptions for Accounting Transactions for Funds 076 and 523
- Investment Accounting Transactions for Fiscal Month (All funds)
- Cash Receipts Journal Report
- Non-Cash Summary
- Cash Disbursement Journal Report
- Cash Receipts Detail
- Non-Cash Journal Detail
- Cash Disbursements Journal Detail

The analyst accesses TM\$ Document Detail Browse to print the cash documents automatically created by TM\$, to ensure all transactions are completed. A "V" next to a transaction means it was automatically validated and a "C" means it will be manually validated by the Cash Management Division. The fiscal analyst ticks/matches the details to the transaction summaries, the confirmation screen, and the document detail browse amounts.

### Cash Management Division Process

Every afternoon, Vicki Boudia, Banking Services Administrator, or other designated staff, reconciles all of the outgoing payments for investment activity for the day (**Key Control #4 - Existence, Completeness**). Once all wires are confirmed, processed, and settled, Vicki reconciles outgoing payments to TM\$ in an excel template called "Afternoon Reconciliation." It reconciles the total outgoing wire and ACH amounts to the individual wire/ACH transactions. The reconciliation does not net wire transactions. Around 2:00 pm, the Cash Management Division receives the daily automated TM\$ email confirming that all investment activity for the day has settled. The email contains the wire template name, and the account and routing numbers used for the investment activities. TM\$ generates this email once Investment Accounting Staff click the daily confirmation button within TM\$.

Vicki logs into US Bank SinglePoint Application using her password store feature. The application does not require a token ID since there are no wires being initiated or released. Vicki prints the daily outgoing wire report "Current Day Summary and Detail Report" from US Bank Single Point

## State of Washington

and labels each transaction with the corresponding agency. Vicki highlights the dollar amount, agency, receiving bank and other relevant information on the report. Then she validates that the amounts on the wire out report match the documents cash management receives (the memo from accounting, TM\$ email, and EFT JV).

Once Vicki validates all the documents match, she signs the wire out report. Investment staff serve as primary and secondary approvers for all wires and Vicki performs a third review. The reconciliation continues until there are no variances. Finally, Vicki pulls an "ACH Log Browse" Report in TM\$ and confirms that the status of all transactions is "match" and "ack" for acknowledged. Vicki pulls the TM\$ document listing by category for the outgoing payments. She double checks that both a document and bank transaction are verified and entered into TM\$, which then interfaces with AFRS.

### **Day 3 (Prior Day) - Reconciliation** **Investment Accounting Division Process**

Investment Accounting perform the reconciliation of the prior day TM\$ Confirmation Report to Northern Trust Cash Transaction Detail Report using an excel spreadsheet. They receive the "Settled Transactions with Debit Credit" from Northern Trust, which shows the daily investment activity and any outstanding cash balance (which should be zero since the goal is to match inflows and outflows of funds from the account) (Day 2). The fiscal analyst places the information from the Northern Trust report and the TM\$ confirmation screen on a "Cash Balance Reconciliation" spreadsheet, to make sure they agree **(Key Control #5 - Existence, Completeness, Classification)**.

Investment Accounting receives scheduled reports by email from AFRS Enterprise Reporting (ER). Investment Accounting staff review the "AFRS Un-Balanced In-Process Report" for funds 076, 523, and 845. This is in the backup reports package.

They review "AFRS Transaction History," Revenue, & Expenditure reports from ER for the three funds. A fiscal analyst reconciles these reports to TM\$. A fiscal analyst performs a reconciliation of the TM\$ book amount listed for the investments to the amount recorded in AFRS in GL 1205 (Temporary and/or Pooled Cash Investments). The reconciliation compares information from AFRS Enterprise General Ledger Trial Balance Report to the book value on the TM\$ Investment Statement, which involves staff making tick marks on copies of the reports. Staff review the AFRS 4300 GLs (Cash in Custody of State Treasurer) daily by adding the prior day's ending balances from the AFRS General Ledger Trial Balance Reports and compare the total to the TM\$ Fund book balance for the day using the "DlyBalRecon" Spreadsheet. In addition to the daily reconciliation, staff performs a monthly reconciliation for fund 076, 523, and 845 to ensure that the par and market value amount on the monthly Northern Trust Position Report agrees to the monthly investment statement holding report.

### ***Cash Management Division Process***

A fiscal analyst performs a full reconciliation of the previous day's transactions. The fiscal analyst obtains a US Bank Statement from the bank's web site and compares it to the TM\$ Valid Bank Transactions Reconciliation Report Screen for the previous day **(Key Control #5 - Existence, Completeness, Classification)**.

## State of Washington

### **How Transactions are Recorded in AFRS:**

TM\$ automatically prepares vouchers for upload into AFRS. Agency Accounting staff prepare manual JVs for items like miscellaneous bank fees and reimbursements (076). An Accounts Payable staff member creates the JV and the Accounts Payable Manager reviews the JV's daily before releasing them. IT staff upload the automatically prepared accounting documents for the entire agency. On the following day, a fiscal analyst reconciles the AFRS general ledger(s) relevant to cash, the balance-in-process report, and TM\$ to ensure they agree and amounts are posted to the proper account. The Investment Accounting Manager performs a high-level review of this reconciliation, which is also performed at the end of each month.

### **Classification of Investments Between Current and Non-Current at Year-End**

TRE uses GL1205 for all investments throughout the year, which is reconciled daily as described above. At the end of the year, Investment Accounting staff prepare JV's to reclassify investments based on their scheduled maturity date. TM\$ produces the report "Investment Statement for General Ledger Postings" for funds 523 (LGIP), 076 (Concentration), and 845 (SMA). At fiscal year-end, the Investment Accounting Manager and other staff work together to run the TM\$ report, export it into Excel, and review the worksheet to determine if any corrections are needed. Based on the maturity date(s), the report allocates the investments into the following separate categories:

<b>GL 1205</b>	Temporary and/or pooled cash investments-liquid/mature 3 months from purchase (short-term investments)
<b>GL 1209</b>	Short-term portion of long-term investments (maturing by 6/30/2023)
<b>GL 1210</b>	Investments-Maturing past 6/30/2023 (non-current)

Once Investment Accounting staff have determined the correct allocation and made necessary adjustments (if any), they enter a JV in AFRS to apportion the balances among the appropriate accounts. A fiscal analyst prepares and enters the JV and the accounting manager approves and releases the batch. Once released into AFRS, TRE prepares a "Disclosure Form A" with the final amounts, which OFM requires annually. The form allocates investments by type and by maturity (**Key Control #6 - Classification**).

### **Key controls are as follows:**

**Key Control 1 (Existence, Completeness):** Verification of Trade Data – Investment Division staff input data for trades into TM\$ daily. The trade tickets are emailed to Investment Accounting, who check that the information has been entered correctly on the trade verification screen in TM\$.

**Key Control 2 (Existence):** Investment Division Staff initiate and review all incoming and outgoing investment wires.

**Key Control 3 (Existence, Completeness):** Re-verification of activity for today's confirmation and new trades on settlement date - Investment Accounting reconcile a "Projected Cash Detail - Today" report from Northern Trust to the TM\$ "Investment Custody Wires" report. In addition, a daily reconciliation of the TM\$ pre-confirmation report to all of the transactions of the daily investing activities is performed.

## State of Washington

**Key Control 4 (Existence, Completeness):** Afternoon reconciliation of outgoing payments - Cash Management Staff reconcile all outgoing investment activity for the day.

**Key Control 5 (Existence, Completeness, Classification):** Reconciliation of Northern Trust, TM\$, AFRS, and US Bank - Investment Accounting Staff compare various TM\$ reports to Northern Trust reports from the prior day to ensure nothing has been posted to the incorrect fund.

**Key Control 6 (Classification):** Investment Accounting staff allocates investments between current and non-current based on maturity date in TM\$.

### Noted Weaknesses are as Follows:

None noted.

### I.1.PRG - Cash & Investments

*Procedure Step:* Key Control #1 - TM\$ (Manual)

*Prepared By:* SHW, 4/4/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm investment division staff input and verify trade data (key control #1 for TM\$) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.



## State of Washington

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

## **Cash & Investments - Existence, Completeness**

**Key Control #1** - Investment division staff input and verify trade data for TM\$.

The understanding for this system is documented above in the "Controls - TM\$" step.

### **1. Confirmation of Key Manual Control:**

**Key Control 1: Verification of Trade Data – Investment Division staff input data for trades into TM\$ daily. The trade tickets are emailed to Investment Accounting, who check that the information has been entered correctly on the trade verification screen in TM\$.**

#### Investment Division:

We reviewed a Bloomberg trade ticket dated 3/20/24 for US Treasury Notes, Cusip 91282CGPO, Broker = Santander US Capital Market, Settle date = 3/20/24; Quantity = 15,000,000; Principal = \$14,783,789.06; Yield = 4.401362.

TRE staff noted this trade as "45094 Buy Credit 3.20". We traced the trade ticket to the "Daily Ticket Summary" excel spreadsheet where it was combined with purchase 45093 and TM\$ Confirmation Screen. We confirmed that everything matched. ***No issues noted.***

We reviewed the Northern Trust "Projected Cash Detail -Today" report, dated 3/20/24. The report showed the following: 20 Mar 2024, 91282CGPO "UNITED STATES OF AMER TREAS NOTES" Shares 03-19-2024 At a price of \$98.558593 NET AND OTHER CHARGES \$32,608.700, We also reviewed the 3/20/24 TM\$ Trade Verification Screenshot. All transaction information matched. ***No issues noted.***

#### Accounting Division:

We reviewed the trade tickets that the Investment Division emailed to the Investment Accounting Division, dated 3/20/24. The trade tickets include information such as the CUSIP number, broker name, amount, and trade date. We noted that tick marks were made next to each piece of input information (e.g. buy/sell, quantity, principal, and settle date) of the investment on the tickets. We reviewed the Daily Ticket Summary for 3/20/24 and noted it ties to the TM\$ Trade Verification Screenshot. ***No issues noted.***

### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

# State of Washington

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #2 - TM\$ (Manual)

*Prepared By:* SHW, 3/27/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm staff review investment wires (key control #2 for TM\$) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls .Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation.

## State of Washington

Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

## State of Washington

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Cash & Investments - Existence**

**Key Control #2** - Investment Wire Review for TM\$

The understanding for this system is documented above in the "Controls - TM\$" step.

# State of Washington

## **1. Confirmation of Key Manual Control:**

**Key Control 2: Investment Division Staff initiate and review all incoming and outgoing investment wires.**

### Control Walk-Through:

We reviewed the TM\$ Confirmation Screen for 3/20/24 and noted the following wires: Fund 523 - \$5,150,737,444.42 IN and \$5,150,045,050.00 OUT, Fund 076 \$29,671,117.50 IN and \$44,839,888.12 OUT and Fund 456 \$2,550.00 OUT for a net of \$14,478,926.20 OUT.

We reviewed the 3/20/24 TM\$ Investment Custody Wires report and the "Previous Day Summary and Detail" reports from US Bank for the LGIP account and Custodian accounts. The TM\$ Investment Custody Wires report shows outgoing wires to Northern Trust for \$15,171,320.62 from the Concentration Account, \$692,394.42 from the Northern Trust to the LGIP, and \$79,415,000.00 from the Concentration Account for a late day trade. The amounts agree to the days wire confirmation report. We reviewed the confirmation email for the trades that have settled for 3/20/24. Chris Mattoon, Portfolio Administrator, sent the email to the TRE MI Investment Team Mailboxes and noted "All trades have settled. Wires (3) are ready for release, Three more secLend wires are also in need of release" Shawn Reed, Portfolio Manager, replied to the email from Chris Mattoon on the same day noting "Wires approved." This confirmed that the wire was prepared by Chris and approved by a second Portfolio Administrator. We also reviewed the "Projected Cash Detail - Today" report as well as the Northern Trust Settlements Report for 3/20/24, which supported the detail in the wire confirmation report and the total wire out for the day of \$14,478,926.20 confirming amounts have settled. We reviewed the US Bank previous day summary and detail report for 3/20/24 and verified wires were initiated and confirmed by different OST investment division staff. *No issues noted.*

### **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #3 - TM\$ (Manual)

# State of Washington

*Prepared By:* SHW, 4/4/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

**Purpose:**

To confirm staff re-verify daily trade activity and perform a daily reconciliation (key control #3 for TM\$) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated"



## State of Washington

step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider

## State of Washington

whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.

B. Controls are not related to a "significant risk" identified in the audit plan.

C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.

D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Cash & Investments - Existence, Completeness**

**Key Control #3** - Staff re-verify daily trade activity and perform a daily reconciliation for TM\$.

The understanding for this system is documented above in the "Controls - TM\$" step.

#### **1. Confirmation of Key Manual Control:**

**Key Control 3: Re-verification of activity for today's confirmation and new trades on settlement date - Investment Accounting reconcile a "Projected Cash Detail - Today" report from Northern Trust to the TM\$ "Investment Custody Wires" report. In addition, a daily reconciliation of the TM\$ pre-confirmation report to all of the transactions of the daily investing activities is performed.**

Investment Accounting Division staff reconcile a "Projected Cash Detail - Today" report (also called the Settlements Report) from Northern Trust to the TM\$ "Investment Custody Wires" report. We reviewed a daily reconciliation of the TM\$ pre-confirmation report to all of the transactions of the daily investing activities is performed as well as a Trade Verification Screenshot.

## State of Washington

We reviewed a TM\$ Trade Verification Screen that contained trades to be settled on 3/20/24, "Projected Cash Detail - Today" report from Northern Trust for 3/20/24, the "Daily Ticket Summary" report for 3/20/24, and the TM\$ "Investment Custody Wires" report for settlement date 3/20/24. We noted that staff use tickmarks across the Trade Verification Screen and all boxes in the "Verified" column were marked. We confirmed the amounts between the reports tied. Investment Accounting Division performs this comparison to re-confirm the final transaction amounts.

We reviewed the Pre-Confirmation Report from TM\$ that shows information such as the Fund, CUSIP, Trade Date, Settlement Date, Settlement Amount, and Par value. We traced Bloomberg trade ticket for Invoice 45094 to the Pre-Confirmation Report for 3/20/24 and tied the transaction tied to the confirmation screen in TM\$ and the "Projected Cash Detail - Today" report from Northern Trust. ***No issues noted.***

### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #4 - TM\$ (Manual)

*Prepared By:* SHW, 4/5/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To confirm Cash Management Staff reconcile all outgoing investment activity for the day (key control #4 for TM\$) in order to assess control risk.

# State of Washington

## **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

## State of Washington

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

## **Cash & Investments - Existence, Completeness**

**Key Control #4** - Cash Management Staff reconcile all outgoing investment activity for the day for TM\$

The understanding for this system is documented above in the "Controls - TM\$" step.

### **1. Confirmation of Key Manual Control:**

**Key Control 4: Afternoon reconciliation of outgoing payments - Cash Management Staff reconcile all outgoing investment activity for the day.**

**Auditor's Note:** When the daily trades result in a net wire out, TRE staff utilize an EFTJV Recon file to ensure the amounts paid are correct. When the trades result in a net wire in, TRE staff utilize a DIB screenshot and reconcile it against the trades for the day.

We reviewed an email from TM\$ with the subject - "3/20/24 - Daily Confirmation WOST - InvAcct". The email lists details of a wire confirmation with Northern Trust for \$15,171,320.62 out of the Concentration Account and \$692,394.42 from the Northern Trust to the LGIP. We also reviewed the 3/20/24 EFTJV Reconciliation docusigned by Kelly Millner, Fiscal Analyst 2 and approved by Ryan Pitroff, Cash Management Manager. Total bank wires out for the day (\$109,553,330.08) were reconciled to Northern Trust, book transfers, LGIP and agency EFT JV's with \$0 variance. We noted that the amounts on the bank statement and the TM\$ reconciliation matched. We also reviewed the AFRS JV/A8 (24032001) and verified amounts recorded tied to the days activity. *No issues noted.*

### **Noted Weaknesses are as follows:**

None

# State of Washington

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #5 - TM\$ (Manual)

*Prepared By:* SHW, 4/8/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm Investment Accounting Staff compare various TM\$ reports to Northern Trust reports to ensure nothing has been posted to the incorrect fund (key control #5 for TM\$) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

## State of Washington

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood



## State of Washington

of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

# State of Washington

## **Cash & Investments - Existence, Completeness, Classification**

**Key Control #5** - Investment Accounting Staff compare various TM\$ reports to Northern Trust reports to ensure nothing has been posted to the incorrect fund for TM\$.

The understanding for this system is documented above in the "Controls - TM\$" step.

### **1. Confirmation of Key Manual Control:**

**Key Control 5: Reconciliation of Northern Trust, TM\$, AFRS, and US Bank - Investment Accounting Staff compare various TM\$ reports to Northern Trust reports from the prior day to ensure nothing has been posted to the incorrect fund.**

We reviewed the Investment Accounting reconciliation of fund 523 for 3/20/24. The reconciliation verified the daily change (uninvested amount left in the fund at the end of the day) of fund 523 (\$669.29) to custodian (Northern Trust), AFRS, TM\$, and US Bank. We also verified the reconciliation was prepared by Alexis Lopez, Fiscal Analyst, and approved by Allison Mrochek, Fiscal Analyst 2. *No issues noted.*

We reviewed the documents listed in the table below. We noted that AFRS ties to TM\$ Investment Statement balance for Fund 523. Northern Trust daily change agrees to the US Bank Statement. The accounting reconciliation ties the AFRS GLs, TM\$ Fund 523 Investment Statement, Northern Trust, and US Bank daily changes together to ensure that Northern Trust, TM\$, AFRS, and US Bank information is correct. *No issues noted.*

Documents & Accounts	AFRS Subsidiary GL TB	TM\$ 523 Investment Stmt	Settled Transactions (NT)	US Bank Statement	Accounting Reconciliation
<b>AFRS GL 1205</b>	\$22,251,969,813.22	\$22,251,969,813.22			
<b>AFRS GL 4310</b>	\$(2,112,626.36)				\$(2,112,626.36)
<b>AFRS GL 4320</b>	\$2,113,295.65				\$2,113,295.65
<b>Daily Change</b>			\$692,394.42 (net)	\$692,394.42 (net)	\$692,394.42 (net)
<b>Account Balance</b>				\$669.29	\$669.29

**Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

# State of Washington

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #6 - TM\$ (Manual)

*Prepared By:* SHW, 4/8/2024

*Reviewed By:* RKM, 5/6/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm the current and non-current investment determination (key control #6 for TM\$) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls .Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

## State of Washington

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the

## State of Washington

appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Cash & Investments - Classification, Valuation**

**Key Control #6** - Current and Non-current investment determination for TM\$

The understanding for this system is documented above in the "Controls - TM\$" step.

**Auditor's Note: Substantive testing for this key control cannot occur before Phase 2 cut-off in September 6, 2024.**

# State of Washington

## **1. Confirmation of Key Manual Control:**

### **Key Control 6: Investment Accounting staff allocates investments between current and non-current based on maturity date in TM\$**

Our confirmation uses documents retained in the PY audit file under TM\$ Testing, Test 6.

We reviewed the "Investment Statement for General Ledger Postings" for 6/30/2023 from TM\$. It shows information such as the Investment number, CUSIP, Settlement Date, Trade Date, and Days from settlement or trade to maturity. The investments are organized in columns by which ones should remain in GL1205 (where all investments are held throughout the year), or be moved to GL 1209 or GL 1210 (based on maturity date).

GL1205 = Liquid/Mature 3 months from purchase

GL1209 = Maturing by 6/30/2023

GL1210 = Maturing past 6/30/2023

If investments have been allocated to the incorrect column, staff will mark the report and deduct or add amounts to the total at the end of the report. The report we looked at had check marks next to the GL account totals verifying they were the correct amounts to be allocated.

We reviewed the AFRS JV "A7-A" used to reallocate the funds. We tied the following transaction details to the "Investment Statement for General Ledger Postings":

1209v/1205 – Fund 076 - \$7,131,602,834.59

1210v/1205 – Fund 076 - \$10,021,581,729.43

1209v/1205 – Fund 523 - \$11,953,807,957.68

1210v/1205 – Fund 523 - \$1,040,955,363.66

1209v/1205 – Fund 845 - \$244,598,134.34

1210v/1205 – Fund 845 - \$736,256,671.61

The JV is marked as prepared by Katie Davis, Fiscal Analyst, on 7/25/23 and signed as approved by Denise Nguyen, Accounting Services Manager, on 7/31/23. *No issues noted.*

### **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

# State of Washington

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.1.PRG - Cash & Investments**

*Procedure Step:* Risk Assessment - TM\$

*Prepared By:* SHW, 9/18/2024

*Reviewed By:* RKM, 9/30/2024

Purpose/Conclusion:

#### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

1. Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to a material misstatement, assuming that there are no related controls. Inherent risk can be thought of as the "threat" of misstatement. Inherent risk exists independently of control risk (the level of threat exists independent of the level of vulnerability to threats). Consider the following factors as your basis for this assessment:*

#### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

*Inherent Risk due to Error*

## State of Washington

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*· Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

2. Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and testing (if applicable). If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*In order to set control risk to LOW, general controls would also need to be tested to provide evidence of the consistent operation of automated controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*



## State of Washington

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body.*

***All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

3. Assess the risk of material misstatement for each relevant assertion for each material line item. The risk of material misstatement is a combination of the auditor's separate assessment of inherent and control risk.

*The Risk of Material Misstatement is a combined assessment of inherent and control risk based on auditor's judgment. If inherent and control risk are assessed differently, it is a matter of professional judgment as to whether the combined assessment is moderate or if one factor outweighs the other.*

4. Design a substantive testing strategy that addresses the relevant assertion in all significant transaction streams included within the material line item.

*In addition to identifying what to audit (material balances) and what to audit for (relevant assertions), planning has also identified how much to audit (risk of material misstatement). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria.7

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done.7

### **(1) Inherent Risk (IR):**

## State of Washington

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Existence - **High**  
Completeness - **Mod**  
Classification - **High**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

Existence - **MAX**  
Completeness - **MAX**  
Classification - **MAX**

We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Existence - **High**  
Completeness - **Mod**  
Classification - **High**

### **(4) Testing Strategy:**

Considering the relevant assertions and risk of material misstatement we developed a substantive testing strategy. We also considered AU-C Section 501.A1-.A4 regarding sufficient and appropriate audit evidence for "Investments in Securities and Derivative Instruments". The State Treasurer's portfolio consists primarily of short term high quality securities reported at fair value. There are no derivatives or collateralized mortgage obligations and debt securities are reported as Level 2 with observable inputs including quoted prices for similar securities and interest rates.

We plan to perform the following tests:

Confirm the balances for Fund 076, Fund 523, and Fund 845 in TM\$ with the amount recorded at US Bank at year-end (Existence).  
Confirm par and fair value amounts for Fund 076, Fund 523, and Fund 845 in TM\$ with the amount recorded in Northern Trust at year-end (Existence).

# State of Washington

Recalculate the investment income and accrued revenue amounts to ensure accuracy, completeness, and reliability of TM\$ (Completeness).

Reconcile the balances for Fund 076, Fund 523, and Fund 845 in TM\$ with the amounts recorded in AFRS at year-end (Completeness, Existence).

Reconcile the aggregate amount of cash in general ledger numbers 4310 and 4320 to the Treasurer's cash balance in TM\$ at year-end (Completeness, Existence).

Review year-end journal entries for the apportionment of cash between current and long-term investments (Classification).

**Note:** Cash and Investments in the Treasurer's Local Government Investment Pool (LGIP) are reported in a stand alone financial statement which will be audited by a CPA firm and reliance will be placed on that audit.

See work performed here: [Work of Other Auditors - LGIP](#)

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## I.1.PRG - Cash & Investments

*Procedure Step:* Controls - Restricted C&I

*Prepared By:* SHW, 4/9/2024

*Reviewed By:* RKM, 4/30/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

## State of Washington

1. List the financial statement balances and relevant assertions addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.

In gaining an understanding of controls, consider the overall understanding of COSO elements as documented in the "Entity-wide COSO Evaluation" step as they relate to this particular system.

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or ACFR AIC if you identify different systems than the ones anticipated in the Matrix.

### **For each material system, auditors must document:**

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

**A brief outline of the transaction flow from beginning to end.**

**An expanded description of key controls.**

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

When (or how often) is the control applied

Who or what initiates the control

Who performs the control

To the extent needed, the experience, knowledge and attitude of the person applying the control

## State of Washington

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any alternative processing or exceptions to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

Internal controls for the **worksheet adjustments** address the following balance(s):

## **Restricted Cash and Investments**

Governmental Activities - GOV - Opinion Unit  
Fund FAA - General Fund - Opinion Unit  
Fund FBG - Higher Education Special Revenue Fund - Opinion Unit  
Aggregate Remaining Funds - NON- Opinion Unit

For the following assertion:

**Classification** - OFM as the financial statement preparer may be unaware of restrictions placed on cash and investments based on information in AFRS.

## **Gain an Understanding of Internal Controls**

We met with Laura Lopez, Statewide Consultant, on April 3, 2024, to review OFM's process of accounting and reclassifying restricted cash and investments.

OFM State Wide Accounting requires **all** state agencies complete a year-end "Cash and Investments Restricted Disclosure" to determine the classification of all cash and investments not available in current operations or restricted for a specific purpose (**Key Control 1- Classification**).

AFRS loads data into the disclosure form application each night, which automatically prefills the GL data for certain forms, including the Cash and Investment Restricted disclosure form. The [disclosure form](#) includes the following sections:

- Question 1 - Prefills Account and amount for GL Code 1140 (Restricted Cash and Investments-Current Operations) at June 30
- Question 2 - Prefills Account and amount for GL Code 1240 (Restricted Cash and Investments- Non-Current) at June 30
- Question 3 - Prefills Account and amount for AFRS in GL Code 1150 (Cash with Fiscal Agents) at June 30
- Question 4 - Unspent Bond Proceeds: Amounts are not prefilled but contain data in dropdown boxes. The disclosure form contains the following dropdown GLs: 1110, 1120, 1205, 1206, 1209, 1210, 4310.
- Question 5 - Other Externally Restricted Cash & Investments: Agencies holding funds for balances and accounts outside of these sections (other externally restricted cash and investments held outside the state treasury) must provide the account, GL Code, amount and nature of the external restriction.

Agencies complete the disclosure form online. OFM provides instructions on how to complete the form in [SAAM 90.40.20](#).

# State of Washington

Laura Lopez initiates an analytical pre-review of the related GLs before agencies begin submitting disclosure forms. The analysis includes certifying AFRS data to ensure the forms are complete and accurate (**Key Control 2 - Classification**). She reviews the composition of the balances then reviews unusual GL information. Laura also reviews submitted disclosure forms to ensure the information provided is complete and that the balance is properly restricted or should be restricted based on the agency's explanation. Each agency head or CFO must certify that the statements listed are true for their agency on the "Financial Disclosure Certification" form (**Key Control 3 - Classification**). The certification process includes affirming AFRS data and any other statements are accurate and complete. See [SAAM 90.40.95](#) for the certification. If Laura determines that an agency needs to prepare a disclosure, she contacts the agency to have them prepare and sign it. Sara Rupe, Deputy Statewide Accounting Director, and Anna Quichocho, Statewide Accounting Manager, review the final fund statements to ensure classification is correct (**Key Control 4 - Classification**).

## **How Transactions are Recorded in AFRS:**

Based on the analysis described above, OFM performs a worksheet adjustment outside of AFRS. OFM manually adjusts the fund statements and does not upload them to AFRS because adjustments work in conjunction with the data provided by AFRS. OFM uses WDesk, a program that has separate columns to include AFRS amounts, adjustments made, and new amounts (AFRS + adjustments). If OFM identifies an error before prior to Phase 2 financial closure, they request that the agency makes a correction in AFRS.

## **Summary of Key Controls**

**Key Control 1** - OFM State Wide Accounting requires all state agencies complete a year-end "Cash and Investments Restricted Disclosure" to determine the classification of all cash and investments not available in current operations or restricted for a specific purpose

**Key Control 2** - Prior to the receipt of all disclosure forms, a fiscal analyst (Laura Lopez) starts an analytical pre-review of the related GLs. This includes certifying AFRS data to ensure the forms are complete and accurate.

**Key Control 3** - Each agency head or CFO must certify that their statements listed are true for their agency on the Financial Disclosure Certification form.

**Key Control 4** - The final fund statements are reviewed by Sara Rupe, Deputy Statewide Accounting Director, and Anna Quichocho, Statewide Accounting Manager, to ensure classification is correct.

## **Noted Weaknesses are as follows:**

None noted.

## **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #1 - OFM (Manual)

# State of Washington

*Prepared By:* SHW, 4/3/2024

*Reviewed By:* RKM, 4/30/2024

Purpose/Conclusion:

**Purpose:**

To confirm Cash & Investment Restricted Disclosures (key control #1 for AFRS) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated"



## State of Washington

step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider

## State of Washington

whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.

B. Controls are not related to a "significant risk" identified in the audit plan.

C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.

D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Restricted Cash & Investments - Classification**

**Key Control 1** - Cash & Investments Restricted Disclosure for AFRS

The understanding for this system is documented above in the "Controls - Restricted C&I" step.

#### **1. Confirmation of Key Manual Control:**

**Key Control 1** - OFM State Wide Accounting requires **all** state agencies complete a year-end "Cash and Investments Restricted Disclosure" to determine the classification of all cash and investments not available in current operations or restricted for a specific purpose.

This control confirmation uses documents from the previous fiscal year.

We viewed the [disclosure form](#) for agency 540 (Employment Security Department) for fiscal year 2023 using the following criteria: Enterprise Reporting, Financial Reports, Disclosure Reports, State, Cash/Investment, Restricted Cash and Investments. We noted that GL Code 1150 totaled \$3,367,209,993. OFM determined the funds were correctly classified. ***No issues noted.***

# State of Washington

We reviewed all agencies Financial Disclosure Certification Forms submissions as part of the FY23 audit at B.2.5 and found all agencies submitted the appropriate and required disclosures. ***No issue noted.***

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.1.PRQ - Cash & Investments**

*Procedure Step:* Key Control #2 - OFM (Manual)

*Prepared By:* SHW, 4/8/2024

*Reviewed By:* RKM, 4/30/2024

Purpose/Conclusion:

### **Purpose:**

To confirm Analytical pre-review of related GLs (key control #2 for AFRS) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

## State of Washington

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

## State of Washington

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

## **Restricted Cash & Investments - Classification**

**Key Control 2** - Analytical pre-review of related GLs for AFRS

The understanding for this system is documented above in the "Controls - Restricted C&I" step.

### **1. Confirmation of Key Manual Control:**

**Key Control 2** - Prior to the receipt of all disclosure forms, a fiscal analyst (Laura Lopez) starts an analytical pre-review of the related GLs. This includes certifying AFRS data to ensure the forms are complete and accurate.

Based on a conversation with Laura on 4/8/24 she indicated that she performs this procedure but does not maintain any documentation unless an issue is found. We confirmed follow-up procedures are performed in the test of disclosure forms as part of the FY23 ACFR audit at B.2.PRG.

### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #3 - OFM (Manual)

*Prepared By:* SHW, 4/3/2024

*Reviewed By:* RKM, 4/30/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm Agency Restricted Cash & Investment Certification, key control #3 for AFRS, in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent

## State of Washington

material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.



## State of Washington

C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.

D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Restricted Cash & Investments - Classification**

**Key Control 3** - Agency Restricted Cash & Investment Certification for AFRS

The understanding for this system is documented above in the "Controls - Restricted C&I" step.

#### **1. Confirmation of Key Manual Control:**

**Key Control 3** - Each agency head or CFO must certify that their statements listed are true for their agency on the Financial Disclosure Certification form.

We reviewed the State Financial Disclosure Certification form as part of FY23 year-end audit procedures at B.2.5 **No issues noted.**

We plan to review those filings again for FY24 at [\[Phase II Planning\]](#).

#### **Noted Weaknesses are as follows:**

None

#### **2. Preliminary Control Risk Assessment**

## State of Washington

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

#### **I.1.PRG - Cash & Investments**

*Procedure Step:* Key Control #4 - OFM (Manual)

*Prepared By:* SHW, 4/3/2024

*Reviewed By:* RKM, 4/30/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm Final Fund Statement Review (key control #4 for AFRS) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls .Inquiries,

## State of Washington

inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

## State of Washington

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Restricted Cash & Investments - Classification**

**Key Control 4 - Final Fund Statement Review for AFRS**

# State of Washington

The understanding for this system is documented above in the "Controls - Restricted C&I" step [[Controls - Restricted C&I](#)].

## **1. Confirmation of Key Manual Control:**

**Key Control 4** - The final fund statements are reviewed by Sara Rupe, Deputy Statewide Accounting Director, and Anna Quichocho, Statewide Accounting Manager, to ensure classification is correct.

We reviewed controls over financial statement preparation as part of the FY23 ACFR audit at L.1.PRG. **No issues noted.**

We will review and confirm internal controls over financial statement preparation for the FY24 ACFR at [[Financial Statement Preparation](#)].

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.1.PRG - Cash & Investments**

*Procedure Step:* Risk Assessment - Restricted C&I

*Prepared By:* SHW, 8/28/2024

*Reviewed By:* RKM, 8/29/2024

Purpose/Conclusion:
---------------------

## **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

1. Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to a material misstatement, assuming that there are no related controls. Inherent risk can be thought of as the "threat" of misstatement. Inherent risk exists independently of control risk (the level of threat exists independent of the level of vulnerability to threats). Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

## State of Washington

*· Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

2. Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and testing (if applicable). If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*In order to set control risk to LOW, general controls would also need to be tested to provide evidence of the consistent operation of automated controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body.*

***All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

3. Assess the risk of material misstatement for each relevant assertion for each material line item. The risk of material misstatement is a combination of the auditor's separate assessment of inherent and control risk.

*The Risk of Material Misstatement is a combined assessment of inherent and control risk based on auditor's judgment. If inherent and control risk are assessed differently, it is a matter of professional judgment as to whether the combined assessment is moderate or if one factor outweighs the other.*

4. Design a substantive testing strategy that addresses the relevant assertion in all significant transaction streams included within the material line

## State of Washington

item.

*In addition to identifying what to audit (material balances) and what to audit for (relevant assertions), planning has also identified how much to audit (risk of material misstatement). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Classification – **High**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

#### **Restricted Cash & Investments (Classification) – MAX**

**MAX** – We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:



# State of Washington

## Restricted Cash & Investments (Classification) – High

### **(4) Testing Strategy:**

Based on our assessment of the risk of material misstatement, we plan to perform the following tests:

Obtain year-end cash and investment disclosure forms and verify restricted amounts are properly reported in the proper GL.  
Obtain and review worksheet adjustments prepared by OFM restricting cash or investments in the governmental or business-type activities, general fund, and aggregate non-major opinion units.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **I.1.PRG - Cash & Investments**

*Procedure Step:* Substantive Tests

*Prepared By:* CJM, 11/19/2024

*Reviewed By:* CJG, 11/21/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

Existence: To determine whether reported cash and investments existed as of the end of the period.

Completeness: To determine whether the financial statements report all cash and investment balances held as of the end of the period.

Classification: To determine whether the financial statements properly classify cash and investment balances in conformity with generally accepted accounting principles (GAAP).

#### **Conclusion:**

Existence: We determined reported cash and investments existed as of the end of the period. ***No issues noted.***

Completeness: We determined whether the financial statements report all cash and investment balances held as of the end of the period. ***No issues noted.***

Classification: We determined whether the financial statements properly classify cash and investment balances in conformity with generally

## State of Washington

accepted accounting principles (GAAP) except for accrued interest of \$35,378,092.08 improperly classified as interest receivable rather than cash and investments. E: OST Investment Fair Value Excludes Interest Aggregation of Misstatements (GAAP)

Testing Strategy:

**Add the testing strategy for each relevant assertion from the TeamStore.**

### **SAO Policy Requirement: Confirming or Verifying Cash & Investment Balances**

Confirmations can either be blind or a positive confirmation. In a blind confirmation (sweep), the auditor requests information on all accounts the bank holds for the entity (by entity name and/or EIN). In a positive confirmation, the auditor lists accounts (or accounts and balances) per the entity and asks the bank to confirm that the information is correct.

Confirm cash and investment account balances with County Treasurer, bank and/or brokerage. Use the template confirmation form provided in the Store when needed.

Confirmations can be mailed to addresses listed on the Bank Confirmation Address List available on the Auditor Reference Guide. If the bank notifies you of a different address, please contact Team Audit Support to update the list.

Banks may confirm incorrect amounts either due to a simple mistake, use of a wrong confirmation date or incorrectly including or excluding accounts. The first step in resolving differences should be to check information against the entity's bank statements and then call the bank to specifically confirm any difference.

Confirming investments may involve physical inspection, confirmation with the issuer, confirmation with the custodian, confirmation of unsettled transactions with the broker/dealer, confirmation with the counterparty, and/or reading executed partnership or similar agreements. When confirming investments, ensure investments are held in the entity's name.

*If confirmations are not used*, auditors must at minimum verify balances to the County Treasurer, bank and/or brokerage statements. If this is done, the auditor should consider the risk that the statements were altered and should examine papers for indications of alteration.

The following is a list of **additional considerations** for testing the existence assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Bank Reconciliations**

If the auditor is comparing reconciled (confirmed) bank or county treasurer balances to the GL (rather than confirmed amounts within an expected variance due to reconciling items), the auditor should consider performing some or all of the following tests to verify the accuracy of the reconciliations. Note that testing the reconciliation will provide evidence of both the existence and completeness of cash and investment balances.

## State of Washington

Trace (or compare summed) bank balances per statements to reconciliations.

Trace (or compare summed) book balances per reconciliations to the general ledger or financial statements.

*If a cash account is allocable to a particular fund, the balance in the general ledger should be recorded in the same fund.*

Scan the reconciliation for reasonableness. Look for unusual, unexpected or vaguely described reconciling items, lack of support or detail, very large reconciling items, very old reconciling items, and missing or extra elements that would indicate that the reconciliation was being performed incorrectly.

Foot the reconciliation for accuracy.

Trace deposits in transit to the subsequent month's bank statement, considering reasonableness of the in-transit period.

Trace outstanding checks to cash disbursement journal.

Check that any other reconciling items are valid and have been properly accounted for (ex: large debit or credit memos).

Check reconciliation against prior and/or subsequent reconciliations for reasonableness of amounts and items included and to trace reconciling items from the previous and/or subsequent period.

### Other Tests

Inquire whether any checks or deposits were being held at year end for budget, cash flow or other purposes.

Confirm investments purchased but not received as of year-end

Confirm investments sold but still held as of year-end

Confirm interest due or accrued but not yet received as of year-end

Search for manual journal entries that debit (increase) cash. Consider testing if risk indicators are noted.

Review reconciliations of clearing and transmittal accounts.

See accountability steps for testing strategies related to petty cash and imprest funds, which are not expected to be material to the financial statements.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

-----  
The following is a list of **considerations** for testing the completeness assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

# State of Washington

## Completeness of Confirmed Accounts

When testing completeness of confirmed accounts, specifically consider the following accounts that are most often missed:

- Accounts related to bond reserves or bond payments

- Accounts related to subsidiary entities or fiduciary funds

- Transmittal accounts (sometimes called "depository accounts") where funds are deposited and periodically "swept" to the main bank account. This is associated most often with property management (with Housing Authorities) and for certain County Treasurers.

- Clearing accounts (also known as "zero-balance accounts" because the expected reconciled balance is zero) related to AP or payroll. Most entities use at least one such account (for federal payroll tax payments).

- In large entities, accounts opened in the name of the department or in the name of a departmental program.

Obtain a list of all bank and investment accounts as of FYE from the entity.

- Scan the list for expected new accounts as a result of new activity (ex: bond issuance) or new process (ex: switching from centralized to decentralized receipting processes).

- Inquire with selected departments to ensure that there are no other accounts that had been opened by the departments.

Compare the entity-prepared list to the prior audit and confirm all accounts that were open last year but closed during the audit period. Inquire of appropriate entity personnel as to when the account was closed, and the reason for closing the account (which may indicate the opening of other new accounts). To verify, obtain final bank statement showing zero balance and any correspondence from the bank confirming the account closure.

Perform a bank sweep by sending blind confirmations to banks that the entity uses and other local banks (confirmations requiring the bank to list all accounts, rather than confirm the entity's list).

## Other Tests

Consider whether the government has any unreported cash and investments, including security or other deposits, held by fiscal agents, vendors, related parties or other governments as part of joint projects or programs.

Confirm investments purchased but not received as of year-end.

Confirm interest due or accrued but not yet received as of year-end.

Search for manual journal entries that credit (decrease) cash. Consider testing if risk indicators are noted.

## State of Washington

Scan bank accounts during the last month of the fiscal year for unusual transactions, particularly on the last day of the fiscal year. If large bank transfers are noted, trace to the bank reconciliation to ensure these are properly accounted for.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

-----

The following is a list of **considerations** for testing the rights and obligations assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Legality of Deposits and Investments**

See steps located in the Accountability cabinet under Assets | Investments sub-folder for testing strategies related to the legality of deposits and investments.

### **Ownership and Encumbrances**

Verify names on accounts through confirmation requests.

Review any contracts or agreements related to the bank account or funds to ensure the account is owned by the entity or if it is only held in trust (if so, it should be presented as a restricted asset with an offsetting liability or as a fiduciary fund, depending on the nature of the arrangement).

Inquire regarding any compensating balance agreements.

*Compensating balance agreements are where an entity contractually agrees to hold a certain amount of money on deposit with a bank, usually at a reduced interest rate, as a condition for approval of a loan.*

If applicable, evaluate whether negative cash or investment balances or overdrawn accounts represent instances of noncompliance (for example, prohibitions against interfund borrowing).

Ensure that refundable deposits held by the entity (such as security deposits) are accounted for as a restricted asset and offset by a liability.

### **Investment Pools (if applicable)**

Check that investment pools are properly established by interlocal agreement (other than the State Treasurer's LGIP which is established by statute).

## State of Washington

Consider whether the government's policy for valuing investments might result in one fund benefiting another based on its method for allocating interest revenues within the pool.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

-----

The following is a list of **considerations** for testing the rights and obligations assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Legality of Deposits and Investments**

See steps located in the Accountability cabinet under Assets | Investments sub-folder for testing strategies related to the legality of deposits and investments.

### **Ownership and Encumbrances**

Verify names on accounts through confirmation requests.

Review any contracts or agreements related to the bank account or funds to ensure the account is owned by the entity or if it is only held in trust (if so, it should be presented as a restricted asset with an offsetting liability or as a fiduciary fund, depending on the nature of the arrangement).

Inquire regarding any compensating balance agreements.

*Compensating balance agreements are where an entity contractually agrees to hold a certain amount of money on deposit with a bank, usually at a reduced interest rate, as a condition for approval of a loan.*

If applicable, evaluate whether negative cash or investment balances or overdrawn accounts represent instances of noncompliance (for example, prohibitions against interfund borrowing).

Ensure that refundable deposits held by the entity (such as security deposits) are accounted for as a restricted asset and offset by a liability.

### **Investment Pools (if applicable)**

Check that investment pools are properly established by interlocal agreement (other than the State Treasurer's LGIP which is established by statute).

## State of Washington

Consider whether the government's policy for valuing investments might result in one fund benefiting another based on its method for allocating interest revenues within the pool.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

-----  
***Auditors are required to contact the Investment Specialist** if they note any **Alternative Investments** [potentially reported at NAV (as a practical expedient)], investments valued at **Level 3** in the fair value hierarchy, or investments with significant interest rate, illiquid level 2 measurements, or other risks with the government's deposits or investments. These types of investments are at higher risk of material misstatement and auditors must perform specific procedures required by standards when applicable.*

The following is a list of **considerations** for testing the valuation assertion for cash and investments. As the valuation assertion for investments often involves greater auditing considerations due to the complexity of measuring investments, the audit approach can vary significantly depending upon the fair value measurements used and the associated risk of material misstatement based on the results from planning procedures (inherent and control risk assessments) which are the basis to the auditor's design of substantive tests. The valuation method used for the measurement or disclosure (for example, cost, equity method, or fair value, and hierarchy level) is a significant factor in properly designing tests of valuation.

### Valuation of Investments

#### **Auditors can utilize three possible audit approaches to testing fair value measurements:**

Develop an independent fair value estimate (generally more effective for Level 1 measurements).

Trace amounts reported for selected or sampled investments to quoted market prices.

Test management's estimation process (generally more effective for Level 3 and the least liquid Level 2 measurements or when management's process already incorporates all of the relevant and reliable valuation sources that are available). Evaluate methodology and support for investments where fair market value is not determined by quoted market prices.

Determine whether the entity's policies for valuing its investments are in conformity with GAAP and appropriately applied to investments.

Test how management made the accounting estimate and the data on which it is based (including valuation techniques used by the entity in its valuations). Test the operating effectiveness of the controls over how management made the accounting estimate, together with appropriate substantive procedures.

## State of Washington

Develop a point estimate or range to evaluate management's estimate (auditor might decide to develop a point estimate or range to evaluate management's point estimate if the auditor (a) is not able to obtain an understanding of the process used to generate the price, including controls over the process of how reliably the price is determined, or (b) does not have access to the model, including the assumptions and other inputs used).

Test subsequent events and transactions (evidence of subsequent purchases, sales or other relevant transactions has to be available).

Determine whether events occurring up to the date of the auditor's report provide audit evidence regarding the accounting estimate.

A government may use quoted prices provided by third parties, such as pricing services or brokers, **if the government has determined that those prices are developed in accordance with GASB 72.**

The following list pertain to potential audit approached to gain evidence regarding information from third-party pricing sources used by management:

For level 1 inputs, comparing the information from third-party pricing sources with observable market prices (reputable online sources)

Reviewing disclosures provided by third-party pricing sources about their controls and processes, valuation techniques, inputs, and assumptions

Testing the controls that the user management has in place to assess the reliability of information from third-party pricing sources

Performing procedures at the third-party pricing source to understand and test the controls and processes, valuation techniques, inputs, and assumptions used for asset classes or specific investments of interest

Evaluating whether the prices obtained from third-party pricing sources are reasonable in relation to prices from other third-party pricing sources, the entity's estimate, or the auditor's own estimate

Evaluating the reasonable of valuation techniques, inputs, and assumptions

Developing a point estimate or range for some investments priced by the third-party pricing source and evaluating whether the results are within a reasonable range of each other

Obtaining a service auditor's report that covers the controls over the validation of the prices\*

### **Investment Pools (if applicable)**

Determine whether pool investments are reported at fair market value, unless a governmental external investment pool operates in conformity with GASB 79 p. 4, or if the external investment pool operates by policy consistent with SEC's Rule 2a7 for regulated money markets (a 2a7-like pool), in which case investments may be reported at amortized cost.

Review or recalculate allocation of gains, losses and investment expenses from pooled cash and investments to individual funds invested in the pool (internal investment pool).

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to*



# State of Washington

*the Financial Statements step*

## **Valuation Related Disclosures**

In accordance with GASB 72 p. 80, valuation and related disclosures required should be organized by type of asset or liability. The following should be taken into consideration when determining the level of detail and disaggregation and how much emphasis to place on each disclosure requirement:

- The nature, characteristics, and risks of an asset or a liability

- The level of the fair value hierarchy within which the fair value measurement is categorized

- Whether a GASB standards specifies a type for an asset or a liability

- The objective or the mission of the government (disclosures should distinguish between the primary government and its discretely presented component units.)

- The characteristics of the government

- Relative significance of assets and liabilities

- Whether separately issued financial statements are available

- Line items presented in the statement of net position

The following are among the required note disclosures related to investments at fair value:

- For recurring and nonrecurring fair value measurements:

  - Fair value measurement at end of reporting period

  - Fair value hierarchy level (except for investments that are measured at the NAV per share)

  - Descriptions of valuation techniques used

  - Change in valuation technique, if applicable, that has a significant impact on measurement, including the reason for making the changes

- For nonrecurring fair value measurements, the reason for the measurement

## State of Washington

Policy for determining which investments, if any, are reported at amortized cost

For any investments in external investment pools that are not SEC-registered, a brief description of any regulatory oversight for the pool and whether the fair value of the position in the pool is the same as the value of the pool shares

Any involuntary participation in an external investment pool

If an entity cannot obtain information from a pool sponsor to allow it to determine the fair value of its investment in the pool, the methods used and significant assumptions made in determining that fair value and the reasons for having had to make such an estimate

Any income from investments associated with one fund that is assigned to another fund

---

The following is a list of **considerations** for testing the classification assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Classification between Line Items**

Verify that amounts have been properly classified as cash, cash equivalents or investments on financial statements (see policy/criteria tab for definitions).

Verify that externally restricted amounts are classified as restricted

### **Classification between Opinion Units**

Search for manual journal entries that transfer cash from one opinion unit to another without recording an operating statement transaction (debit and credit to cash and fund balance for each opinion unit, respectively). Consider testing if any risk indicators are noted.

Search for manual journal entries that re-classify existing cash balances (transaction is a debit and credit to different cash accounts). Consider testing if any risk indicators are noted.

Compare budgeted interest earnings to actual and follow-up on any significant difference.

Calculate an estimated implied interest rate for each opinion unit by dividing interest earnings by the average of beginning and ending cash and investment balances. Compare across opinion units and follow-up on unexpected results.

Review cash transfers or journal entries that move cash without debiting an expenditure to determine if cash was improperly moved.

# State of Washington

Check that any suspense funds were reported at 0 as of fiscal year end (per [BARS 3.6.11](#)).

Scan titles of fiduciary funds and follow up with additional procedures to verify the nature of any funds that appear to be misclassified.

## **Presentation of Overdrawn Balances**

Determine whether overdrawn cash balances are properly reported as liabilities rather than as negative cash balances.

Determine whether interfund balances are properly recorded for overspent or over-committed agency funds.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

Guidance/Criteria:
--------------------

**Add the Guidance/Criteria for each relevant assertion from the TeamStore. You may also include other resources that you used for testing.**

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Outstanding Checks and Deposits in Transit** – Per TIS section 1100.08 (AICPA Technical Questions and Answers), outstanding checks should be reported as a reduction of cash and the amount of deposits in transit should be reported as cash. A check is considered outstanding from the time that it is out of the payor's control – when mailed or delivered to the payee – until the time it clears the bank. Cash should represent amounts within the control of the reporting entity, that is, the amount of cash in banks plus cash and checks on hand and deposits in transit minus the amount of outstanding checks.

**SAO Audit Policy [6350](#) – External Confirmations**

**[Investments](#) Area Guide**

**[LGIP Fund Summary Reports](#)** - includes a list of local government accounts and balances in the Local Government Investment Pool

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

# State of Washington

## **BARS [3.8.6](#) Use of Payroll and Claims Funds**

---

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

[Investments](#) Area Guide

[LGIP Fund Summary Reports](#) - includes a list of local government accounts and balances in the Local Government Investment Pool

[Bank Confirmation Address List](#)

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

## **BARS [3.6.11](#) Suspense Funds**

## **BARS [3.8.6](#) Use of Payroll and Claims Funds**

---

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

Violations of investment laws should be disclosed per GASB 3 par 66 and GASB 38 par 9.

[Investments](#) Area Guide

[LGIP Fund Summary Reports](#) - includes a list of local government accounts and balances in the Local Government Investment Pool

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

## **BARS [3.8.6](#) Use of Payroll and Claims Funds**

[GASB 3](#) Deposits with Financial Institutions, Investments (Including Repurchase Agreements), and Reverse Repurchase

# State of Washington

**Agreements** - paragraph 66 "Significant violations during the period of legal or contractual provisions for deposits and investments ... and the actions taken to address such violations should also be disclosed. ..."

## **GASB 38 Certain Financial Statement Note Disclosures**

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

GASB 72 paragraph 69, as amended, requires all investments be measured at fair value except as follows:

- Investments in nonparticipating interest-earning investment contracts (such as nonnegotiable certificates of deposit) – Cost-based measure (see GASB 31, p. 8.)

- Investments in unallocated insurance contracts – Reported as interest-earning investment contracts

- Money market investments and participating interest-earning investment contracts with remaining maturity at time of purchase of one year or less and are held by governments other than external investment pools – Amortized Cost

- Investments held by qualified external investment pools – Amortized Cost

- Investment in qualified external investment pools – Amortized cost (governmental external investment pool meets criteria of GASB 79, p.4)

- Synthetic guaranteed investment contracts (SGICs) that are fully benefit responsive – Contract value

- Investments in life insurance contracts – Cash surrender value

Fair value measurements should be made consistent with the provisions of GASB Codification *3100 Fair Value Measurement*.

### **Valuation Methods**

To measure fair value, GASB 72 p. 18, requires governments to use valuation techniques that are appropriate in the circumstances and for which sufficient data are available, maximizing the use of observable inputs and minimizing the use of unobservable inputs. A government should use one or more of the following three approaches to measure fair value (GASB 72 p. 23-27):

- Market Approach – uses prices and other relevant information generated by market transactions involving identical or similar assets, liabilities, or groups of assets and liabilities. Techniques consistent with market approach are include:

  - Quoted market prices

  - Market multiples technique

  - Matrix pricing technique

- Income Approach – converts future amounts (i.e. cash flows or revenues and expenses) to a single current (discounted) amount.

When the income approach is applied, the fair value measurement reflects current market expectations about future amounts.

Valuation methods consistent with the income approach include:

# State of Washington

Present value techniques

Option pricing models

Multi-period excess earnings methods

Cost Approach – reflects the amount that would be required currently to replace the present service capacity of an asset. Fair value is determined based on the cost to a market participant (buyer) to acquire or construct a substitute asset of comparable utility, adjusted for obsolescence.

Governments may invest in a variety of investments –fix income securities (i.e. asset backed securities), exchange-traded equity securities, government investment pools, and alternative investments (i.e. private equity funds, hedge funds, real estate) (pension and endowment funds). The valuation assertion often involves greater auditing considerations due to the complexity of measuring investments. The audit approach will vary significantly depending upon the fair value measurements used and the associated risk of material misstatement. The valuation method used for the measurement or disclosure (cost, equity method, or fair value) is a significant factor in properly designing tests of valuation.

## Investments Area Guide

[LGIP Fund Summary Reports](#) - includes a list of local government accounts and balances in the Local Government Investment Pool

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.8.6](#) Use of Payroll and Claims Funds**

### **[GASB Codification 3100](#) Fair Value Measurement and Application**

---

#### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Cash** - Consistent with common usage, cash includes currency on hand, demand deposits, and deposits in other kinds of accounts that have the general characteristics of demand deposit accounts in that the government may deposit additional cash at any time and also effectively withdraw cash at any time without prior notice or penalty (SGAS 9, footnote 5).

**Cash Equivalent** – Defined by GASB Codification 2450.106 as short-term, highly liquid investments that are both (a) readily convertible to known amounts of cash and (b) so near their maturity that they present insignificant risk of changes in value because of interest rates; generally only investments with original maturities of three months or less (at time of purchase) meet this definition. Original maturity means the original

## State of Washington

maturity to the entity holding the investment. For example, both a three-month U.S. Treasury bill and a three-year Treasury note purchased three months from maturity qualify as cash equivalents. However, a Treasury note purchased three years ago does not become a cash equivalent when its remaining term is three months. [GASB 9, fn 6]

**Restricted Cash and Investments** – Cash and investments should be classified as restricted whenever externally imposed restrictions (those imposed through law or by creditors, grantors, contributors or regulations of other governments) change the normal understanding of the availability of the asset. For example, a normal understanding of cash and investments is that the government is not limited in its ability to use the cash and investments to pay current liabilities (GASB 34 par 34 and 99).

### Investments Area Guide

**LGIP Fund Summary Reports** - includes a list of local government accounts and balances in the Local Government Investment Pool

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS 3.2.2 County's External Investment Pool** (*applies only to counties*)

**BARS 3.6.11 Suspense Funds**

**BARS 3.8.6 Use of Payroll and Claims Funds**

Record of Work Done.:
-----------------------

**Test 1: Confirm the balances for Fund 076 Concentration, Fund 523 LGIP, and Fund 845 SMA, in TM\$ with the amount recorded by US Bank as of June 30, 2024**  
**(Existence)**

We obtained and reviewed the bank reconciliations performed by Ryan Pitroff, Banking Services Manager, Cash Management Division, for all three funds at 6/30/2024. See bank reconciliations and TM\$ Balance Summaries for Fund 076 Concentration Tests 1-5, Concentration Account Bank Recon, 523 LGIP Tests 1-5, LGIP Account Bank Recon and 854 SMA . We tied the balances of each fund to the corresponding US Bank statements for each account, see here: OST Test 1. We compared the balance per US Bank, to the balance in the TM\$ balance summaries, and as shown on the bank reconciliation worksheet for each account. We selected the largest positive and negative reconciling items, amounting to 83.5% of the total, to do further testing on. See summary of coverage selection and detail of testing on the Fund 076 reconciliation worksheet here: . **We confirmed that**

## State of Washington

**the reported balances for Fund 076 Concentration, Fund 523 LGIP and Fund 845 SMA existed as of 6/30/2024 per TM\$ and US Bank. No issues noted.**

**Test 2: Confirm investments tie between Northern Trust and TM\$ and to confirm the par and market value amounts for Fund 076, Fund 523, and Fund 845 in TM\$ with the amount recorded at Northern Trust and outside banks as of June 30, 2024 (Existence):**

See testing performed at [OST Test 2](#) & holding statements at [Test 2 ReconInvestmentStatementJune2024](#) for Funds 076, 523, and 845 to reconcile total investment balances at par and market value(s) per TM\$ to the Custodian Bank at 6/30/2024. We obtained the Northern Trust Asset Detail and identified securities reported in TM\$ that were not reported on the asset detail. We obtained bank statements from Katie Davis, Fiscal Analyst to confirm that all reported investments in TM\$ valid support from an entity apart from the Treasurer's office. [Test 2 - Bank Statements](#) We agreed amounts to statements and noted the last 4 digits of the account number in the reference column on our reconciliation. Katie Davis also provided us with the time deposit excel spreadsheet, the Linked Deposit Program spreadsheet and the LGIP CD tracking spreadsheet to agree amounts for the CD, TCD and Linked Deposit accounts. **We determined that TM\$ contains a complete list of investments between what is reported by Northern Trust and banks holding cash investments. We confirmed that par and market value amounts for Fund 076, Fund 523 and Fund 845 agreed to the amounts recorded with Northern Trust as of June 30, 2024 except for an issue related to the par and fair value of investments not including interest paid on 6/30 totaling \$35,378,092.08 As a result interest and dividends receivable were overstated and cash and cash equivalents were understated.** [E: OST Investment Fair Value Excludes Interest](#)

**Test 3: Verify investments in the custody of Northern Trust includes accrued revenue at June 30, 2024 which agrees to TM\$ (Completeness):**

We used the substantive sampling spreadsheet to determine our sample size, linked here: [OST Test 3](#). We used the TM\$ Accrued Revenue Statements for Fund(s) 076, 523, and 845 to select a sample of 38 investments in order to recalculate their accrued interest revenue. See detailed calculation methodology within our referenced work paper for the different types of securities. We excluded bank account deposits because the interest cannot be computed in auditor recalculations due to daily fluctuations in account balance. We cross referenced selected investments to the TM\$ Investment Statements for Fund(s) 076, 523, and 845 at [Test 3 Investment Statmtent for GL Postings 2024 June 30](#). We recalculated accrued interest revenue on selected investments at: [OST Test 3](#) tab "Testing".

Some of the selected securities are "Floating Rate Notes," which have a variable rate of return. These securities have "FRN" as part of the security description. Due to the complexity of the formula to determine accrued revenue, we obtained charts showing how OST calculated the accrued revenue daily. We cross referenced the Investment Number selected for testing against the Investment Statement (Sorted by Security Class Number) [OST Test 3](#) to obtain the CUSIP and confirm the security class. We used the security class tab [OST Test 3](#) to gain greater detail on how the security's accrued interest is calculated (Prime or SOFR Floater).

Details about Treasury Note FRNs can be found here: <https://treasurydirect.gov/marketable-securities/floating-rate-notes/>. The interest rate is the sum of the highest accepted discount rate of the most recent 13-week Treasury bill with a "spread" rate, which is fixed for the life



## State of Washington

of the FRN. The interest rate changes weekly. **We recalculated the accrued interest by using the earnings per \$100 interest payment period from the Treasury website and multiplying it by the note face value.**

Details about the SOFR rate (Secured Overnight Financing Rate) can be found here: [<https://www.newyorkfed.org/markets/reference-rates/sofr>]. The SOFR can change daily. **Our samples did not contain investments using the SOFR this year.**

Details about the US prime rate can be found here: [<https://fred.stlouisfed.org/series/PRIME>]. The interest rate changes as the Federal Reserve sets the federal funds target rate. **We noted that for notes using the prime rate that the book yield rates changed on days where the Federal Reserve changed the federal funds target rate.**

**We determined that TM\$ is performing the accrued interest rate correctly for SOFR and Prime calculations as evidenced by changes in the book yield rate. We will rely on the calculation tables as a recalculation for SOFR and Prime note securities.**

We performed our recalculation for the accrued revenue of 38 investments with no variances from the amounts that were calculated by TM\$, ignoring rounding in the recalculations. No further work necessary. *No issues noted.*

### **Test 4: Reconcile balances for Fund 076, Fund 523, and Fund 845 in TM\$ with the amount recorded in AFRS at year-end and Disclosure Form A- Investment Disclosures (Completeness, Existence)**

We reconciled the investment balances for each fund reported in TM\$ with balances reported in AFRS, and Disclosure Form A (Investment Disclosures). See testing performed at: OST Test 4. We ran AFRS queries to obtain the AFRS balances for Funds 523, 076, and 845. See tab "2024 AFRS Investment Balance(s)". We obtained the Investment Disclosures from Katie Davis, Fiscal Analyst. We included the Disclosure Form A for each fund within the OST\_Test\_4 spreadsheet, see tab(s) "2024 Inv Disclosure 523/076/845". We linked amounts on the "2024 Reconciliation" tab directly to supporting numbers on the Disclosure Form (Book Value) and AFRS queries. We also included the Investment Statements for 6/30/2024 from TM\$ for all Funds to ensure they also agreed to Disclosure Form A. See tab(s) "2024 Fund 523/076/845 GL" in the above referenced work paper. **We were able to reconcile the balances for Funds 076, 523, and 845 (Completeness, Existence) without exception. No issues noted.**

### **Test 5: Reconcile the aggregate amount of cash in GL's 4310 and 4320 to the Treasurer's cash balance in TM\$ at year-end (Completeness, Existence)**

We obtained the aggregate amount of cash in GLs 4310 -Current Treasury Cash Activity, and 4320 -Beginning Treasury Cash Balance Admin Agency, from the FY24 ACFR database. We then reconciled the aggregate amount of cash in GLs 4310 and 4320 for all agencies and all funds with the amount of cash reported by OST. See detailed testing performed here: OST Test 5.

We reconciled the total Treasury and Treasury Trust cash reported on the Statement of Receipts and Disbursements for the State Treasury with

## State of Washington

the amounts reported in AFRS for GLs 4310 and 4320. Fund(s) 076 and 523 are not included in the Treasury's Receipts and Disbursements Report, so we subtracted the amount of cash in Fund 076 (Treasury/Trust fund) and Fund 523 (LGIP) from the aggregate amount of cash in GLs 4310 and 4320. We linked AFRS amounts on the "Reconciliation" tab directly to supporting amounts from AFRS queries. Ending book balance for Treasury and Treasury Trust Funds was \$19,363,177,988.69. Total reported in AFRS excluding Fund(s) 076 and 523 was \$19,363,177,988.69. **We were able to determine that reported cash and investments existed as of the end of the period, without exception. No issues noted.**

We also reconciled the amount of cash reported in GLs 4310 and 4320 with the amount of cash held in the concentration account (Fund 076). We began with the aggregate amount of cash in GLs 4310 and 4320 and added the outstanding warrants reported on the Statement of Receipts and Disbursements Test 5 Receipts and Disbursements June 2024. We subtracted the LGIP cash balance in AFRS of \$911.90 and cash on hand in the amount of \$65,233.16 per the Daily Cash on Hand Activity Report at: Test 5 Cash on Hand FY 24. We subtracted bank errors in the amount of 26,703.32 per TM\$: Test 4 Concentration TM\$ Accounting Recon Screen. The remaining difference was explained by reviewing Ryan Pitroff's June 2024 reconciliation for the concentration account: Tests 1-5, Concentration Account Bank Recon. We removed agency deposits recorded by OST as of July 1st and added in NSF adjustments, bank adjustments, and the physical deposit exception. See detailed testing performed here: OST Test 5. We reconciled the aggregate amount of cash in GL's 4310 and 4320 to the Treasurer's cash balance in TM\$ at year-end (Existence) without exception. **No issues noted.**

### **Test 6: Review year-end journal entry to ensure investments were properly allocated between short-term and long-term (Classification)**

We obtained and reviewed the AFRS JV #090IN019 dated 7/26/24 OST Test 6 and traced allocation amounts to GL 1209 and 1210 to the corresponding investment statements for Fund(s) 076, 523, and 845 (also included in Test 6 Apportion Investments FY24 see total amounts on pages 24, 29, and 43). Allocation balances agreed to the totals reported for each GL on the Investment Statements. We also ran an AFRS query and compared the total(s) by GL and fund number. See testing performed at: OST Test 6 **We confirmed that investments were appropriately classified between short term and long-term at June 30, 2024 (Classification). No issues noted**

### **Restricted Cash & Investments: Obtain year-end cash and investment disclosure forms and verify restricted amounts are properly reported in the proper GL (Classification)**

See testing performed at: OST Restricted Cash Testing. We obtained a list of worksheet adjustments from OFM and placed the fund statement adjustments in the "2024 Worksheet Entries - Fund" tab and government-wide adjustments in the "2024 Worksheet Entries GovtWide" tab. We sorted entries to filter out increases to sort codes AF and/ or DM for fund level entries, and 1H and 1S for government wide restricted cash and investments. We also obtained a disclosure report for restricted cash and investments from Enterprise Reporting: Financial Reports, Disclosure Reports, State, Cash/Investment, and then selected the report titled "Cash and Investments-Restricted Cash and Investments". We ran the report and added it to our work papers at tab "Disclosure 2024".

We performed the following procedures to ensure worksheet adjustments were supported by corresponding disclosures:

## State of Washington

1. We traced each fund level worksheet adjustment that increased restricted cash and investments (sort code AF) to supporting disclosures in sections 3, 4 and 5 of the Restricted Cash and Investments Disclosure Report, which is used to report cash with fiscal agents (GL 1150), unspent bond proceeds, and other externally restricted cash and investments. See tabs "2024 Worksheet Entries - Fund" [OST Restricted Cash Testing](#) and "Disclosure 2024" [OST Restricted Cash Testing](#)
2. We reviewed line items from the Disclosure Report that were not reclassified per the OFM worksheet to ensure they meet the definition of restricted cash (per GASB 62) and ensure they were not incorrectly omitted. See [GASB 62, paragraph 31](#), for definition. We determined that balances were properly reported. **No issues noted.**
3. We tied the worksheet adjustments at the government-wide and business-type level to the corresponding fund-level worksheet entries. Government -wide and business-type activities worksheet adjustments that increased sorts codes 1H were traced to the totals of the fund-level worksheet entries. See tab "2024 Worksheet Entries GovtWide" [OST Restricted Cash Testing](#) **No issues noted.**

### **Restricted Cash & Investments: Obtain and review worksheet adjustments prepared by OFM restricting cash or investments in the governmental or business-type activities, general fund, and aggregate non-major opinion units (Classification)**

See testing performed at: [OST Restricted Cash Testing](#). To verify that restricted amounts are properly reported, we obtained the restricted cash and investment disclosure report from Enterprise Reporting and performed the following procedures:

1. We ran an ACFR query for sort code(s) AF and DM. See tab "2024 Query AF, DM" [OST Restricted Cash Testing](#). We summarized the balances at the rollup fund level. See tab "ACFR Restricted Rollup Fund 24" [OST Restricted Cash Testing](#). We compared the balance for each rollup fund to the corresponding disclosures on section 1 of the disclosure report to ensure amounts agree. **No issues noted.**
2. We added the fund-level worksheet adjustments for each rollup fund, to the amount disclosed in section 1 of the disclosure report (GLs 1140 and 1240), and tied amounts reported for each opinion unit on the financial statements [\[2024 ACFR for SAO Version No. 1 11.15.2024\]](#) at: [\[OST Restricted Cash Testing\]](#). See tab "ACFR Restricted Rollup Fund 24."

### **Reconciliation to Material Account Matrix**

We performed additional procedures to reconcile the balances audited at OST to the Final Significant Account Matrix [Final Planning Significant Account Matrix](#) Cash and Investment balances. See [OST Recon Significant Account Matrix](#) for testing. Our detailed understanding is documented below.

#### **A. Sort Code AC**

We ran a query in the FY24 ACFR database for sort code AC by GL account number including all funds and performed a reconciliation to determine the total cash balance covered by auditor procedures at the State Treasury and the total audited as part of other procedures. See the "FY24 Summary\_AC" tab in our workpaper [OST Recon Significant Account Matrix](#) . By running the AC query by detail agency, we separated the

## State of Washington

balances into the following categories:

### **B. Sort Code(s) AM and DJ**

**Audited at OST** (54% of balance)- All balances for agency 090 including totals for GLs 4310 (Current Treasury Activity) and 4320 (Beginning Treasury Cash Balance Admin Agency) which were reconciled as part of our substantive testing at OST (Test 5). At year-end, OST makes an adjustment to allocate the fair value gain to receipt funds at the rollup level in GL 1280-Valuation Allowance-Investments. We reviewed the adjustment obtained from Katie Davis, Fiscal Analyst, and ran a query using the FY24 ACFR Database to confirm the total fair value gain. See tab "OST JV090IN023" in our workpaper for details:  
OST Recon Significant Account Matrix.

**OFM year-end adjustments** at the rollup fund level (64% of balance) At year-end OFM does a number of adjustments to allocate balances at the rollup fund level. Adjustments over \$5 million are reviewed as part of Financial Statement Preparation at:  
Adjustments.

**SIB Accounts** audited by other CPA: A portion of the balance (-18% of the balance) was attributable to the State Investment Board. (The negative cash, due to owner funds, is cleared in OFM agency 700 year-end adjustments) These balances are audited by an outside CPA firm, and we will rely on their work at: Work of Other Auditors - SIB

**Worker's Compensation Funds-** A portion of the balance (-0.02%) was audited as part of the Worker's Compensation Audit at S1WorkersCompensationFunds-FS24.

**Not reconciled at OST-** (0.02% of the balance) - Not in the custody of the State Treasurer. The remaining balance is comprised of amounts not included in the Treasurer's balance audited at OST. See column I on tab" FY24 Summary\_AC" in our workpaper:  
OST Recon Significant Account Matrix. GLs 1130 and 1150 are by definition not funds in the custody of the State Treasurer. Transactions in the "in-process" accounts are considered outstanding until they are cleared by OST and adjusted to GL 4310. Balances in these accounts are not recorded by the State Treasurer and represent outstanding transactions that agencies must include as reconciling adjustments in tying their cash balances to OST.

In total, we concluded that the amount of \$31,662,728,669 on the final significant account matrix for Sort Code AC is covered by audit procedures. This represents 98% of the balance. **No issues noted.**

### **B. Sort Code(s) AM and DJ**

We ran additional queries for sort codes AM and DJ for all funds at agency 090 by GL account number. The balances in AM and DJ consist primarily of funds in the Treasury Income Account (Fund 076) and the Public Investment Account (Fund 523). A small portion of the total was attributable to allocations to GL 1280 and 1216. We were able to tie balances from our query to the Significant Account Matrix for the corresponding GL sort codes. See tabs "FY24 AM\_Detail" and "FY24 DJ\_Detail" in our workpaper for details. **No issues noted.**

# State of Washington

## I.2.PRG - Non Depreciable Assets

*Procedure Step:* Summary & Conclusion

*Prepared By:* NJH, 10/17/2024

*Reviewed By:* RKM, 11/19/2024

Purpose/Conclusion:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In

# State of Washington

making this determination, auditors should evaluate:

## Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

## **I.2.PRG - Non Depreciable Assets**

*Procedure Step:* Understanding of Line Item

*Prepared By:* NJH, 6/10/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.



## State of Washington

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria:

Record of Work Done:

### **(1) Prior Audit Exceptions:**

None.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

Each year we review the two most recent fiscal year data due to timing between when the audit was started and when the CY ACFR database is available. This allows us to gain an understanding of the line item based on the most relevant data available at the time of beginning the audit.

#### Balance Breakdown for 2023/2022

We reviewed the balances for fiscal years 2023 and 2022 and determined that the line item balance was composed of five account balances. Of these accounts, 93% were covered within the GL account 2120, fund 997, which is Land and Other Non-Depreciable Assets. GL account 2120 is made up of the transportation infrastructure including highways, bridges, tunnels, and safety rest areas. Assets are recorded using the modified approach, which requires assets to be maintained at levels set by the agency and verified by biennial inspections/assessments. The assets are grouped into three categories: Pavement, Bridges, and Safety Rest Areas.

Related to this account there are three balances related to maintenance expenses. As of FY2023, 96.4% are broken out between pavements (57.4%) and bridges (39%).

During our control understanding with Pavements on 5/21/24 and Bridges on 5/22/24 we inquired about any major changes. Both informed us there were no major changes with pavements and bridges in FY24.

# State of Washington

## **(3) Updates to Significant Account Matrix:**

None

## **I.2.PRG - Non Depreciable Assets**

*Procedure Step:* Controls - CPMS/TRAINS/WSPMS

*Prepared By:* NJH, 8/20/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion.:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy.:

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.  
In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.  
Identify controls systems covering all relevant assertions for all significant classes of transactions.  
Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

## State of Washington

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented. Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

## State of Washington

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **Material Balance and Assertions:**

# State of Washington

Internal controls in the CPMS/TRAINS/WSPMS address the following balance(s):

Non Depreciable Assets

For the following assertions:

Valuation - There is a risk that the Washington State Legislature is not sufficiently funding infrastructure for the DOT to perform preservation maintenance. There is a risk DOT is reporting infrastructure using the modified approach when it should be reported using the historical cost approach because average preservation thresholds are not met. Governmental activities capital assets would be incorrectly valued and presented (depreciation would not be reported). Net position would be incorrectly valued. An error would cause an overstatement in the accounts.

Classification - There is risk the state is not adequately maintaining the state highway system and the assets are misclassified as non-depreciable rather than depreciable assets.

## **Gain an Understanding of Internal Controls**

We met with the following DOT staff on to gain an understanding of internal controls over Non Depreciable Assets:

Pavements - Meeting held on 5/21/24

Karen Strauss, State Pavement Management Engineer

Jianhua Li, State Pavement Management Engineer

Jesse Daniels, WSDOT Audit Liaison

Bridges - Meeting held on 5/22/24

Evan Grimm, Bridge and Structures Engineer

Gyung-Seop Shim, Bridge Management Engineer

Roman Peralta, Bridge Preservation Engineer

Jesse Daniels, WSDOT Audit Liaison

## **Pavement**

### **Data Collection**

WSDOT Pavement condition assessment data collection only takes place when there are dry road conditions from April through mid-October. The same lane on each roadway is reviewed each year to determine the deterioration over time to know when those roads need maintenance. The data collection, assessment, and reporting processes begin when the roads are consistently dry enough to measure (usually sometime in March or April) and the assessment for the year will start almost immediately afterward because data is coming into the office every week. The field data collection involves three staff from the pavement team: two for the distress van and one for the friction vehicle. One staff member remains in the office and begins the review of the distress videos. After the data collection is completed and the weather does not allow for collection, the field collection team assists with the review of distress videos in the office. The Pavement Management Unit works to complete the review process

## State of Washington

during the spring of the following year so the final report to the FHWA, DOT Gray Notebook, and the financial statement can occur by the fiscal year end for the previous calendar year assessment. For this year, the Pavement Office is currently working with the 2023 collection data and expect it to be available during the summer of 2024.

Data collection is done by WSDOT Materials Laboratory Technicians utilizing a pavement distress data collection van and a friction measurement vehicle. The distress collection van collects data several ways using the Pathway system which is the pavement software program used by the Washington State Pavement Management System (WSPMS) that is on the pavement collection vans. While driving over at least one lane of all highway routes each year the van collects data in both directions on divided highways. The vehicle continuously measures the depth of rutting and roughness using laser measurements. The International Roughness Index (IRI) or laser data collection, is required to be reported to the Federal Highway Administration (FHWA) annually and they also calibrate the laser annually. There are digital video cameras that take pictures, with views provided from the driver's view, view of the edge of the roadway, a downward facing camera, and a 3D detailed close-up of the lane width of the road. The 3D images are used to see cracking and takes a photo every 26 feet. This data is recorded on a portable hard drive which is removed when the vehicle comes back to the office, either nightly (for local collection) or at least weekly (for trips far from the office). In the Materials Lab, the hard drive data is downloaded to servers in the office for analysis. All data is broken up into 2-hour sections (sets). The friction vehicle tests approximately half the state each year, divided roughly by east and west sides of the state. The friction testing vehicle consists of a truck, which has a large water tank and a friction trailer towed by the truck that measures the friction and reports it to a computer in the truck cab. The friction is measured using a locked wheel trailer with a rubber tire and water applied to the roadway. The driver will press a button and water out of a large water tank in the trailer will come out in front of the tire and an immediate reading will display in the truck. The friction measurements are taken every mile on all highway routes (both directions if divided). The truck also measures friction on bridge decks for special projects and High Friction Surface Treatment areas (HFSTs). This data is recorded in the vehicle and brought in daily (if local), or at least weekly (if not local), to download onto servers. If the driver notices friction reading below the threshold, he will circle around and drive the area again to ensure the reading was correct. If he determines the reading is accurate and below the threshold, it will be immediately reported and sent to the regional office. An internal policy requires immediate action from the regional office because conditions are considered unsafe. Each year, the data is summarized. Any friction measurements below the minimum are reported to the region traffic, materials, and maintenance engineers immediately by the Pavement Unit staff during collection season.

### Reporting, Rating, & Classification

Pavement is classified as either very good, good, fair, poor, or very poor for three separate metrics: The roughness, based on the IRI (International Roughness Index), the rutting of the roadway, and the cracking in the pavement surface. The roughness & rutting data collected by the distress collection van via the pathway system is assigned a rating by the Washington State Pavement Management System (WSPMS), while the cracking is initially analyzed by a DOT pavement engineer and then assigned a rating by the WSPMS. Additionally, the friction truck and trailer measures the friction, but is not used in determining the modified approach to infrastructure. Karen noted that for reporting purposes, cracking is the leading indicator of when pavement needs to be assessed for repairs/additions and is the primary criteria used internally and externally for reporting the pavements condition. The following is the assessment criteria thresholds from the FY23 ACFR RSI on Infrastructure:

Category	PSC	IRI	Rutting
----------	-----	-----	---------

## State of Washington

Very Good	80 - 100	< 96	< 0.24
Good	60 - 79	96 - 170	0.24 - 0.41
Fair	40 - 59	171 - 220	0.42 - 0.58
Poor	20 - 39	221 - 320	0.59 - 0.74
Very Poor	0 - 19	> 320	> 0.74

The data from the data collection vehicle recorded by the Pathway System is stored on physical hard drives and uploaded into the WSPMS system every night in the DOT Material Laboratory. WSPMS has internal formulas and proprietary code that translates the raw collection data into about 1/10 of a mile segments or "preservation units" all initially given the highest criteria rating for each area. WSDOT, like many other DOT state agencies in the US, can set quantitative metrics for good, fair, or poor and a sliding scale to correspond with those metrics. Karen noted that, as an example, Idaho uses a 1-5 scale for rating each of these individual areas while WSDOT uses 0-100 for PSC, 0-500 for IRI, & 0.00-1.00 for rutting as shown in the figure above. For roughness, rutting, & cracking, the WSPMS has backend mathematical formulas and code that transforms the raw data collected from the collection vans to calculate the PRC (Pavement Roughness Condition), the PPC (Pavement Profile Condition - Rutting), and the PSC (Pavement Structural Condition) into numerical values and then subtracts those values from each of the upper limit for each criteria rating to get the final values for each criteria and then categorically assigned a qualitative rating of either very good, good, fair, poor, or very poor **(Key Control #1 - Automated Software Calculation - Valuation/Classification)**. For cracking, prior to a PSC value assigned, an experienced DOT pavement engineer will scan & review the 3-D images and pictures recorded from the collection van and will analyze each video segment and note when they see a crack/inconsistency in the pavements surface. They will note it in the pathway system using "Asphalt Concrete Pavement (ACP) Hot Keys" and "Portland Cement Concrete Pavement (PCCP) Hot Keys" **(Key Control #2 - Manual - Classification)**. When cracking assessment is completed, the raw data is assigned a PSC value in the WSPMS system by translating the hot key inputs entered by the rater and subtracting the aggregated values from 100 to arrive at the final value for cracking. Once all three criteria are assigned a PRC, PPC, or PSC value by the WSPMS system, the WSPMS system has backend system code with logical tests to categorically assign a qualitative rating of either very good, good, fair, poor, or very poor to each pavement section for each criteria. The WSPMS system is only accessible by selected DOT staff within the Pavement department and given certain read/write capabilities as it pertains to the backend code that is responsible for calculating the different criteria values and ratings. Vyenna Kynull, IT App Development Sr/Sc, is the only Pavement staff with access to the code as of FY24, and maintains a log of updated changes or historical access to the code editor for WSPMS to ensure that no changes were made outside of her designated purview. Additionally, the WSPMS system is only accessible by those who have DOT internal network access and are current staff within the DOT directory as given credentials by the DOT IT Network team **(Key General IT Control - see [Key Control #1 (Automated) - Pavement])**.

Infrastructure Projects

## State of Washington

Karen Strauss, State Pavement Management Engineer, explained that her team is only responsible for the preservation and projects to preserve existing highways and do not have anything to do with capital projects. Karen and Jianhua Li, State Pavement Management Engineer, receive the data and ratings from WSPMS and they provide the regions with the information and ask them to analyze the data and update a list of projects they think are necessary. Karen and Jianhua then discuss the data and the suggestions from regions and they make final needs-based recommendations to send to the Capital Program Development and Management Office (CPDM). The final decision for which projects to fund comes from CPDM and the funding provided from legislation. The Capital Program Management System (CPMS) is where all highway construction (and bridge) projects are entered. The CPDM office receives the recommendations and need from the pavement engineers and once they make a decision to fund a project, the regional offices are then sent instructions to fill out their proposals in CPMS. Karen and Jianhua's pavement team is not involved with CPMS.

### **Bridges**

WSDOT performs inspections (condition assessments) on all vehicular bridges and culverts in excess of 20 feet in length. These same structures under 20 feet are also assessed, but are not governed by the same regulations as ones in excess of 20 feet. Most of these bridges and culverts are inspected on a two-year cycle, with some lower-risk bridges inspected on a four-year interval and some higher-risk bridges inspected on an annual basis. The assessment (condition rating) may determine whether a bridge is high risk or low risk. Special inspections, like those for underwater bridge components, are inspected at least once every five years. Federal Highway Administration (FHWA) gives requirements/recommendations as to when bridges need to be assessed based on previously assessed condition.

WSDOT's bridge inspection program complies with all requirements of the FHWA. The Federal Bridge Inspection standards are specified in the code of federal regulations 23 CFR 650 subpart C. WSDOT has documented its inspection process in the Washington State Bridge Inspection Manual M36-64.13 with the latest version published December 2023. The FHWA performs annual reviews of WSDOT's National Bridge Inspection Program (NBIP). The FHWA has developed 23 metrics that are assessed as part of the compliance reviews. The reviews are completed every calendar year, with the latest one being complete in December 2023.

### Inspections

All inspections are completed by National Bridge Inspector Standards (NBIS) certified inspectors. Bridge inspector names and certification numbers are entered and stored in BridgeWorks, a WSDOT developed application, used to record and document the inspections. Most inspections have a lead inspector and co-inspector, but the lead inspector is the only one required to be certified.

Inspectors give a rating to the primary bridge elements (deck, superstructure, and substructure) or culvert using the NBIS codes. NBIS codes are ranged from 0 (failed/collapsed) to 8 (good) using standards established by FHWA.

After the field inspection is performed, the inspection documentation (pictures, inspection, categories, bridge information, etc.) is entered into BridgeWorks. There is a monthly report sent to supervisors that lists all reports that have been locked, but not scanned so inspectors and supervisors can track the release of reports. The condition assessment procedures listed below are performed on an annual basis to ensure the



## State of Washington

percentage of bridges assessed as "fair or better" is within the guidelines of GASB No. 34 (to allow reporting using a modified approach).

Bridge Preservation Office Engineers review the draft inspection reports to ensure the data is accurate and there were no entry errors. The inspection reports are released in the Bridge Engineering Information System (BEIS) after the review is completed. Reports are required to be reviewed and released within 90 days of the inspection date.

The Bridge Asset management Engineer uses the bridge inspection data to determine network condition. A bridge's overall condition is determined by a national standard established by the FHWA and described in the 23 CFR 515. WSDOT has also developed a [folio](#) that summarizes the information as part of the MAP-21 rules.

The primary NBI code for each of the major bridge elements (deck, superstructure, and substructure) is determined based on the inspection results and in accordance with the table below:

Category National Bridge Inventory Code Description
(NBI code 8 or 7) A range from no problems noted to some minor deterioration of structural elements.
(NBI code 6 or 5) All primary structural elements are sound but may have deficiencies such as minor section loss, deterioration, cracking, spalling or scour.
(NBI code 4 or less) Advanced deficiencies such as section loss, deterioration, cracking, spalling, scour or seriously affected primary structural components

The overall bridge condition code is determined by the lowest code for each of the major bridge elements (deck, superstructure, and substructure). If any major element is coded at "4" or less, the overall bridge condition rating is "poor". If all the primary NBI codes are above a "4", but one or more is a "5" or "6", the overall bridge condition rating is "fair". If all the primary NBI codes are a "7" or greater, the overall bridge condition rating is "good". The culvert condition rating is similar.

The Bridge Asset Management Engineer, Hyung-Seop Shim, compiles the assessments into a summary report with a good, fair, or poor rating for each bridge. The percentage of bridge deck area for each rating is used to determine the percentage of bridges at fair or better and compliance with the modified approach for infrastructure (**Key Control #3 - Manual - Valuation/Classification**).

### How Transactions are Recorded in AFRS:

Projects for Capital Outlays and the need for a project is initiated by technical experts at various divisions who review assessment information and determine a need for repair, maintenance, or replacement of an asset. Needs are transmitted to the Capital Program Development and Management Office (CPDM) which then sends scoping instructions to the regional offices. The regional offices then write proposals based on the

## State of Washington

need and determine the projected scope and cost of the project. Regional offices enter the proposal into the Capital Program Management System (CPMS). The completed proposal is given to the CPDM Office, who is responsible for programming projects that fit within identified capital budgets. The Bridge Management Engineers and Pavement Management Engineers we spoke with are not involved with project decisions and entering into CPMS. They perform the assessments and the decision is made by legislation for which preservation projects to fund.

Based on the information entered into CPMS, the Accounting and Financial Services (AFS) division, with the help of CPDM, determine whether an activity should be capitalized and enter the award into the Contract Administration Payment System (CAPS). CAPS, the mainframe system used for construction project management in the regional offices, maintains payment and administrative information related to ongoing construction contracts and projects. CAPS creates payment vouchers to pay contractors by feeding the data to TRAINS. Data is fed to TRAINS by an overnight automatic interface. The Project Office enters the payment information and the release of payment information into TRAINS and the payment processing is done by a Contract Specialist. A daily CAPS to TRAINS reconciliation is performed by a Contract Specialist and the Accounting and Financial Services Division.

TRAINS automatically records all expenditures in AFRS as transportation expenditures. These are recorded in AFRS via nightly upload. At the end of each quarter, the Transportation Financial Consultant (Beth De Vul) prepares a JV to adjust the transportation expenditure balance for the amounts that should be recorded as non-depreciable assets. Then, the Accounting and Reporting unit performs monthly TRAINS/AFRS fund and GL reconciliations to ensure expenditures are properly classified within AFRS.

We confirmed with Jesse Daniels that what DOT classifies as non-depreciable assets for reporting purposes (bridges & pavement) goes through the same process/channel as capital outlays when it comes to how they are recorded in AFRS & TRAINS. Subsequently, because all capital outlays are tracked in CPMS and are assigned a sub-program and ITC to be reviewed in the Capitalization Matrix and ALL equipment and capital projects are recorded in AFRS as a transportation expenditure, the quarterly JV by Beth De Vul to reclassify each asset/project into the correct account/group is also applicable here to the pavements and bridges to be correctly classified as "non-depreciable" assets.

### Key Controls are as Follows:

**Key Control #1 - (Automated Software Calculation) - Valuation/Classification:** For roughness, rutting, & cracking, the WSPMS has backend mathematical formulas and code that transforms the raw data collected from the collection vans to calculate the PRC (Pavement Roughness Condition), PPC (Pavement Profile Condition - Rutting), and PSC (Pavement Structural Condition) into numerical values and the subtracts those values from each of the upper limit for each criteria rating to get the final values for each criteria and then categorically assigned a qualitative rating of either very good, good, fair, poor, or very poor.

**Key Control #2 (Manual) - Classification:** For cracking, prior to a PSC value assigned, an experienced DOT pavement engineer will scan & review the 3-D images and pictures recorded from the collection van and will analyze each video segment and note when they see a crack/inconsistency in the pavements surface. They will note it in the pathway system using "Asphalt Concrete Pavement (ACP) Hot Keys" and "Portland Cement Concrete Pavement (PCCP) Hot Keys".

**Key Control #3 (Manual) - Valuation/Classification:** The Bridge Asset Management Engineer compiles the assessments into a summary report with a good, fair, or poor rating for each bridge. The percentage of bridge deck area for each rating is used to determine the percentage of bridges at fair or better and compliance with the modified approach for infrastructure.

# State of Washington

## Noted Weaknesses are as Follows:

None

### I.2.PRG - Non Depreciable Assets

*Procedure Step:* Key Control #1 (Automated) - Pavement

*Prepared By:* NJH, 8/22/2024

*Reviewed By:* BM2, 11/20/2024

#### Purpose/Conclusion:

##### **Purpose:**

To determine whether For roughness, rutting, & cracking, the WSPMS has backend mathematical formulas and code that transforms the raw data collected from the collection vans to calculate the PRC (Pavement Roughness Condition), PPC (Pavement Profile Condition - Rutting), and PSC (Pavement Structural Condition) into numerical values and the subtracts those values from each of the upper limit for each criteria rating to get the final values for each criteria and then categorically assigned a qualitative rating of either very good, good, fair, poor, or very poor (**Key Control #1 for WSPMS**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

##### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

#### Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

##### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be

## State of Washington

documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### Software Calculation:

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### Automated Interfaces:

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

## State of Washington

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

# State of Washington

## Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

## Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

## State of Washington

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

#### **Automated Interfaces:**

## State of Washington

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:



## State of Washington

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### Software Calculation:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we*

## State of Washington

*would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

## State of Washington

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

## State of Washington

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent

## State of Washington

on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

# State of Washington

## Software Calculation:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## Automated Interfaces:

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

## State of Washington

- Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.
- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

- If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

- If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.
- If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.
- If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

- Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.
- If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

- If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

## State of Washington

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.



# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Information Technology](#) Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

#### Manual vs. Automated Interfaces

A “manual interface” is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the*

# State of Washington

*following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process

## State of Washington

to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

Permits a user to approve transaction(s) within the software system

The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm

# State of Washington

with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **Non-Depreciable Assets - Valuation/Classification**

**Key Control #1 - (Automated Software Calculation) - Valuation/Classification:** For roughness, rutting, & cracking, the WSPMS has backend mathematical formulas and code that transforms the raw data collected from the collection vans to calculate the PRC (Pavement Roughness Condition), the PPC (Pavement Profile Condition - Rutting), and the PSC (Pavement Structural Condition) into numerical values and the subtracts those values from each of the upper limit for each criteria rating to get the final values for each criteria and then categorically assigned a qualitative rating of either very good, good, fair, poor, or very poor.

The understanding for this system is documented above in the [[Controls - CPMS/TRAINS/WSPMS](#)] step.

## **STEP 1: Understand Automated Key Control**

To gain an understanding of this automated control, we met with Karen Strauss, State Pavement Management Engineer, & Vyenna Kynull, IT App Development Sr/Sc, on 8/20/24. The understanding of this automated key control is documented at [[Controls - CPMS/TRAINS/WSPMS](#)].

## **STEP 2: Confirm Automated Key Control:**

To confirm this automated control we met with we met with Karen Strauss, State Pavement Management Engineer, & Vyenna Kynull, IT App Development, on 8/20/24 and requested a live walk through of the WSPMS code base and backend development environment to ensure the code for calculating different pavement values was in place. Vyenna shared with us the CS Code environment class that holds all of the code for the reporting classifications called "GFPReportBC.cs". within this view we were able to identify a string of "if, else" statements for various classifications. For the "very good" rating for PSC, we were able to view the code as follows:

## State of Washington

```
(if (index>=80){  
    return "Very Good";  
...}).
```

Vyenna then proceeded to explain that the different variables created and used in conjunction with data pulled from the "WSPMS Azure data table" which pulls queries directly from the WSPMS database after the pavement collection data is uploaded to the system every night. We were able to confirm that the automated control is in place and using relevant data pertaining to the control identified. ***No issues noted.***

### **STEP 3: Understand General IT Controls**

To gain an understanding of this automated control, we met with Karen Strauss, State Pavement Management Engineer, & Vyenna Kynull, IT App Development Sr/Scc, on 8/20/24. The understanding of this automated key control is documented at [[Controls - CPMS/TRAINS/WSPMS](#)].

### **STEP 4: Confirm Key General IT Controls**

**Key General IT Control:** The WSPMS system is only accessible by those who have DOT internal network access and are current staff within the DOT directory as given credentials by the DOT IT Network team.

To confirm the general IT control identified at [[Controls - CPMS/TRAINS/WSPMS](#)], we met with Karen Strauss, State Pavement Management Engineer, & Vyenna Kynull, IT App Development Sr/Scc, on 8/20/24. Vyenna performed a walk through of the WSPMS code base and backend development environment. Vyenna shared the WSPMS object explorer that holds all of the databases and indexes within the WSPMS system. The example we reviewed was the "WSPMSSurveyINdexHistory" object that had >30 different tables for various historical log reports. One of these included the data table "hist.WSPMSPinChangeLogHistory" which is a list of all designated WSPMS access pin number changes. We believe this is sufficient evidence of the IT control in place within the WSPMS system and were able to confirm this key control. ***No issues noted.***

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **I.2.PR.G - Non Depreciable Assets**

**Procedure Step:** Key Control #2 (Manual) - Pavement

**Prepared By:** NJH, 8/20/2024

**Reviewed By:** BM2, 11/20/2024

## State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm For cracking, prior to a PSC value assigned, an experienced DOT pavement engineer will scan & review the 3-D images and pictures recorded from the collection van and will analyze each video segment and note when they see a crack/inconsistency in the pavements surface. They will note it in the pathway system using "Asphalt Concrete Pavement (ACP) Hot Keys" and "Portland Cement Concrete Pavement (PCCP) Hot Keys" (**Key Control #2 - CPMS/TRAINS**) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

## State of Washington

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

## State of Washington

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #2 (Classification):** For cracking, prior to a PSC value assigned, an experienced DOT pavement engineer will scan & review the 3-D images and pictures recorded from the collection van and will analyze each video segment and note when they see a crack/inconsistency in the pavements surface. They will note it in the pathway system using "Asphalt Concrete Pavement (ACP) Hot Keys" and "Portland Cement Concrete Pavement (PCCP) Hot Keys".

The understanding for this system is documented above in the [[Controls - CPMS/TRAINS/WSPMS](#)] step.

### **1. Confirmation of Key Manual Control:**

To confirm this key control, we met with Marsha Mawdsley (Transportation Planning Specialist) & Dirk Brier (Transportation Planning Specialist) on 7/1/24 to have them perform a walkthrough of the pavement condition assessment. As noted in our understanding of this control, the pavement collection van uses sensors to record two points of data, the roughness (IRI) and the rutting. Dirk noted that the data is stored local on hard drives on the van and is backed up to the Pathway servers every night where the software reads the sensor data and assigns it a score. The only manual criteria that is scored is the cracking in the pavement. Marsha showed us her screen which had a dash cam view of the road (what the driver was seeing) as well as the view of the pavement itself. There were two pavement windows and Marsha informed us one was a 2-D view showing how the surface looks when it's normally visible and another view which was 3-D showing deeper areas of the pavement not normally visible. The data is stored in Pathway as "sets" and Dirk noted that each set would only ever contain about a maximum of about 120



## State of Washington

miles of pavement to assess. Marsha visually scans each segment, which is every three feet, and notes when she sees a crack/inconsistency in the pavement. She notes it in the pathway system using "Asphalt Concrete Pavement (ACP) Hot Keys" and "Portland Cement Concrete Pavement (PCCP) Hot Keys". We obtained a physical copy of this sheet with all of the hot keys on them for our records. These are a list of hot key commands that tie to certain markings/descriptions she can use when she identifies a crack. For example, she would often use keys N & M which are coded for spalling ratings (high & low).

During the walkthrough, we watched as Marsha inspect PCCP pavement footage collected from the second lane on I-5 South in Tukwila as well as ACP pavement footage collected from the second lane on I-5 South in Lynnwood. We confirmed with Dirk that all of the data assessed by Marsha (or another DOT pavement staff member) from a particular data set of footage will be checked using a random sample of that footage by which he will review the assessment made and determine if it is correct or not. This helps them ensure that the hot key ratings used are continually accurate and that the assessors, like Marsha, are continuing to notice the correct inconsistencies in the pavement. ***From our walkthrough we can confirm that pavement condition assessments are completed to ensure highways are inventoried and assessed to allow reporting using the modified approach for infrastructure. No issues noted.***

### **Noted Weaknesses are as follows:**

**None**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.2.PR.G - Non Depreciable Assets**

*Procedure Step:* Key Control #3 (Manual) - Bridges

*Prepared By:* NJH, 8/20/2024

*Reviewed By:* BM2, 11/20/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm the Bridge Asset Management Engineer compiles the assessments into a summary report with a good, fair, or poor rating for each bridge. The percentage of bridge deck area for each rating is used to determine the percentage of bridges at fair or better and compliance with the modified approach for infrastructure **(Key Control #3 - CPMS/TRAINS)** in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent

## State of Washington

material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. *Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. *Controls are not related to a "significant risk" identified in the audit plan.*

## State of Washington

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #3 (Valuation/Classification):** The Bridge Asset Management Engineer compiles the assessments into a summary report with a good, fair, or poor rating for each bridge. The percentage of bridge deck area for each rating is used to determine the percentage of bridges at fair or better and compliance with the modified approach for infrastructure.

The understanding for this system is documented above in the [[Controls - CPMS/TRAINS/WSPMS](#)] step.

### **1. Confirmation of Key Manual Control:**

To confirm this key control, Hyung-Seop Shim, the Bridge Asset Management Engineer, along with a few members of his team, Roman Peralta & Paul Evans, performed a verbal walkthrough of how the assessment summary report is created and updated for the most recent bridge assessments.

We also received the WSDOT G-F-P Bridge Summary titled "SAOreport2024" from Jesse Daniels, Audit Liaison, on 6/11/24. This report had to be updated and we received a new copy the next day on 6/12/24. We inquired about this update during our walkthrough and Paul Evans noted that a new FHWA revision of the [Specifications for the National Bridge Inventory](#) had slightly revised commentary on how the width is calculated/included in the overall calculation of deck area. We compared & calculated the percentage change in total bridge deck area and found that the overall change was insignificant (0.27%).

Hyung informed us that he uses a query tool through the Bridgeworks (WSBIS) database servers to extract and organize bridge information from

## State of Washington

the Main Bridge Inspection databases. He will query out the WSDOT bridges over 20 feet in length that carry Vehicular Traffic (including Ferry Terminals and Bridges Shared with Border States [Oregon and Idaho]) and classify each bridge condition based on their inspection codes. The resulting summary report is provided for use in the WSDOT Grey Notebook and to allow for staff to report using the modified approach according to GASB-34. Similar to the RSI, the WSDOT Grey Notebook is posted every year but the actual bridge assessments are only completed and updated every two years.

We noted the summary report contains a summary of percentage of bridge deck area in poor, fair, and good condition. For the most recent calendar year under bridge review (2023), it showed that 92.4% of bridges were either in good or fair condition. This information will be updated in the RSI for FY24, as inspections are completed and reported on every two years. We determined bridges are assessed, their condition is rated and the ratings are compiled into a summary report that provides WSDOT the basis for compliance with the modified approach for infrastructure. **No issues noted.**

### **Noted Weaknesses are as follows:**

**None**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.2.PRG - Non Depreciable Assets**

*Procedure Step:* Risk Assessment

*Prepared By:* NJH, 7/2/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion.\*

**Purpose / Conclusion:**

# State of Washington

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

## **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

## State of Washington

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

# State of Washington

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

## **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Valuation - Low

Classification - Low

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

### **CPMS/TRAINS - Valuation/Classification**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**



# State of Washington

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Valuation - Low

Classification - Low

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

Test a sample of bridge assessments from the bridge summary report (with a good, fair, or poor rating given for each bridge) to determine the percentage of bridges at fair or better and compliance with the modified approach for infrastructure (Valuation & Classification).

We will rely on the FY2022 State ACFR work performed over highway pavement assessments to determine whether the review is completed to support compliance with the modified approach (Valuation & Classification).

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## **I.2.PRG - Non Depreciable Assets**

*Procedure Step:* Substantive Test - CPMS/TRAINS/WSPMS

*Prepared By:* NJH, 11/8/2024

*Reviewed By:* RKM, 11/20/2024

Purpose/Conclusion:

## **Bridges:**

### **Purpose:**

To determine whether infrastructure assets are reported at properly valued and calculated amounts. To determine whether financial statements properly classify infrastructure assets in conformity with generally accepted accounting principles (GAAP).

### **Conclusion:**

We determined bridge inspections were completed as required and support valuation of bridge infrastructure using the modified approach. We determined bridge inspections were completed as required and support the classification of bridge infrastructure using the modified approach. **No**

# State of Washington

*issues noted.*

## **Pavement:**

### **Purpose:**

To determine whether infrastructure assets are reported at properly valued and calculated amounts. To determine whether financial statements properly classify infrastructure assets in conformity with generally accepted accounting principles (GAAP).

### **Conclusion:**

We determined pavement was reported at properly valued and calculated amounts. We determined pavement assessments were completed as required and support the classification of pavement using the modified approach. However, we noted one minor issue related to DOT not being in compliance with their two year cycle of assessments. See issue at: [\[V: DOT RSI Modified Approach: Infrastructure - Pavement\]](#).

Testing Strategy:

### **Valuation:**

The following is a list of **considerations** for testing the valuation assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Incorrect Depreciation Calculations**

Perform an analytical review of depreciation expense by type of asset for reasonableness.

Re-calculate depreciation expense for a sample of assets or in conjunction with a test of automated controls (if depreciation is automatically calculated by the system). Consider testing the inputs used for the calculation to determine whether they are reasonable and in line with any applicable policies; i.e. useful life, salvage value, etc. Alternatively, test calculations, extensions and footing of subsidiary records if records are maintained on spreadsheets.

Evaluate capital asset policies for componentization or grouping of assets to determine if it has been consistently followed and will result in a rational method of depreciation. See BARS [3.3.10.150](#) for guidance.

Evaluate estimated useful life and scrap value factors for reasonableness. This test could be done in general (on the government's accounting policies), for selected asset classes or for selected or sampled asset records.

*If testing selected high risk assets, auditors should consider assets that are nearly or fully depreciated (see BARS [3.3.10.130](#)), assets with unusually high or low useful lives for their type, and assets with unusually high scrap values.*

Compare estimated useful lives for assets with replacement schedules / policies and capital budgets.

*We would expect that assets on a regular replacement schedule (such as equipment, vehicles, road surfacing, etc) or that are included for replacement in the capital budget would have estimated useful lives that match the government's replacement plans for the asset.*

# State of Washington

Consider whether the date placed in service for assets is reasonable given when the asset begins being used or is substantially complete as this will have an effect on when depreciation begins. See information in BARS [3.3.10.90](#) about when to move a project out of CIP.

## **Impairment**

Check that the measurement method used for write-offs is in accordance with GAAP (GASB 42.12-15). Review or recalculate the portion of historical cost that should be written off for impaired capital assets. *Note: auditor would normally use the same measurement method used by the government unless it the auditor finds it inappropriate for the circumstances or unallowable under GAAP.*

## **Incorrect Historical Cost of Assets**

Trace recorded cost to supporting documentation. *Note: This test would normally be limited to recent additions, since documentation for historical assets has likely passed the records retention period.*

Evaluate the reasonableness of any estimates of the historical cost of capital assets.

Evaluate the reasonableness and support for any estimates of the acquisition value (per GASB 72) of donated capital assets.

## **Conversion to GAAP**

For governments converting to GAAP reporting, examine valuation method for retroactively reported infrastructure assets and verify that the valuation method used is one of the methods prescribed by the County Road Advisory Board.

## **Modified Approach**

Check that infrastructure is being depreciated unless the modified approach is used. If the modified approach is used, verify that the government has met criteria of GASB 34 par 23-26.

## **Allocation**

On the government-wide statement of activities, review allocation of depreciation for capital assets for governmental funds. Depreciation expense will be reported as a component of the direct expense shown in the statement of activities. Request spreadsheet for allocation.

## **Classification:**

The following is a list of **considerations** for testing the classification assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Assets Reported as the Wrong Category**

Scan asset descriptions to determine if assets appear correctly categorized.

Compare asset classification and descriptions to observations and/or review of supporting documentation.

## State of Washington

Test that assets reported in Construction in Progress have not yet been substantially completed. See BARS [3.3.10.90](#). Consider using the L&I [prevailing wage reporting database](#) to scan for projects that may have been completed during the audit period. Identify any significant surplus assets that the government intends to sell from review minutes and check that these are appropriately classified as "assets held for sale."

### **Assets Reported in the Wrong Opinion Unit**

Scan subsidiary ledgers to see if capital and infrastructure assets appear related to the fund they are reported in. Follow-up on all unexpected assets.

Search for manual journal entries that transfer capital assets from one opinion unit to another without recording an operating statement transaction (debit and credit to capital assets and fund balance for each opinion unit, respectively). Consider testing if any risk indicators are noted.

Consider results of recent physical inventory. Follow up on any discrepancies or missing assets that could have been a result of assets moving between departments/funds.

### **Improper Capitalization of Expenditures**

Inquire as to the types of costs the government capitalizes for purchases, construction, software development (if applicable) or other types of assets. Research and follow-up on any practice that appears in conflict with GAAP or in conflict with policy assumptions underlying estimated useful lives, scrap values or any grouping or componentization methodologies used to capitalize assets.

Review supporting documentation for selected capitalized improvements or repair / maintenance expenses to determine whether capitalization criteria was met and were consistent with policy assumptions underlying estimated useful lives, scrap values and any grouping or componentization methodologies used to capitalize assets. See BARS [3.3.10.150](#) for information regarding componentization of assets.

Review supporting documentation for constructed assets to check that all capitalized costs meet GAAP criteria.

Check that any capitalized costs in connection with pollution remediation meet GASB 49 par 22 exceptions (since costs would normally be an expense against the pollution remediation liability).

Review supporting documentation for software development to check that all capitalized costs meet GAAP criteria.

Check that uncapitalized collections (works of art or historical artifacts) meet GAAP criteria for being expensed.

Guidance/Criteria:
--------------------

### **Valuation:**

#### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

2012 GAAFR page 451 describes generally accepted estimation methods for when the historical cost of an asset is unknown. NOTE: The County Road Advisory Board (CRAB) worked with local governments to develop several methods for valuing historical infrastructure assets when GASB 34

# State of Washington

was implemented.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.3.9](#) Capital Asset Management System Requirements**

**BARS [3.3.10](#) Capital Asset Accounting** - guidance on determining ownership of capital assets.

### **BARS [3.9.2](#) Property Transfers**

GAAP criteria for reporting capital assets

**[GASB Codification Section 1400](#) Reporting Capital Assets**

**[GASB Comprehensive Implementation Guide Chapter 7](#) Basic Financial Statements and Mangement's Discussion and Analysis, sections 7.9-7.21**

## **Classification:**

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

GASB 72 (codified at section 3100) distinguishes between classification as capital assets and investments. Since land, rental properties or other tangible property is not an eligible investment for local governments, we would not expect to see any property reported as an investment. Surplus assets awaiting sale should be classified as "assets held for sale." See GASB 72 par B47 for discussion of multi-use assets, such as a city building with the first floor rented out to retail stores. In such cases, the unit of account should be considered the building as a whole in order for reporting to demonstrate legal compliance for investments.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.3.9](#) Capital Asset Management System Requirements**

GAAP criteria for reporting capital assets

**[GASB Codification Section 1400](#) Reporting Capital Assets**

# State of Washington

## [GASB Comprehensive Implementation Guide Chapter 7](#) Basic Financial Statements and Management's Discussion and Analysis, sections 7.9-7.21

Record of Work Done:

### **Bridges:**

Substantive tests performed to meet the Valuation assertion:

See testing performed and results at [\[Bridge Testing\]](#).

To meet the valuation assertion, we selected a sample of 21 bridges from the G-F-P Bridge Assessment we received titled *SAO Report-2024\_updated deck area* from Hyung-seop Shuim, Bridge Management Engineer for DOT. We used the criteria of "Vehicular bridges/Culverts reported to the NBI (>20 ft long)" which makes up about 80% of all bridges included in the assessment, which we deemed a sufficient coverage amount for the assertion. We then had Hyung update the qualitative and quantitative parameters we created that we deemed necessary to obtain in order to substantiate a conclusion. These parameters include the inspection date, the primary inspector, whether or not the bridge is included in WSBIS software, and the frequency the bridge is inspected. All of these parameters were not originally included in the bridge assessment report we received. We then calculated the next assessment date of inspection needed to determine if the bridge was assessed within the 24 or 48 month inspection cycle using calendar year end 12/31/23 (since assessments are performed on a calendar year basis) as referenced in the [WSDOT Bridge Inspection Manual](#) to be included in the FY24 ACFR Required Supplementary Information (RSI). To meet the valuation assertion, we determined if each bridge selected in our sample was included in the assessment and was assigned an NBI rating of fair or good. We were able to confirm the population was complete on the "Pop. Completeness & Tie Out" tab by comparing the total WSDOT reported bridges with the number of bridges reported to the NBI > 20ft that received a rating. We determined that the population used for sampling had an overall rating of "Fair" or better for 94% of the bridges. There was no variance noted within the population, and we consider the population complete for testing purposes. To meet the valuation assertion, we determined if each bridge selected in our sample was included in the assessment and was assigned an NBI rating of fair or good.

Based on our evaluation of results and sampling risk, we determined the sample provided a reasonable basis for conclusions about the population. We determined bridge inspections were completed as required and support valuation of bridge infrastructure using the modified approach. ***No issues noted.***

Substantive tests performed to meet the Classification assertion:

See testing performed and results at [\[Bridge Testing\]](#).

To meet the classification assertion, we selected a sample of 21 bridges from the G-F-P Bridge Assessment we received titled *SAO Report-2024\_updated deck area* from Hyung-seop Shuim, Bridge Management Engineer for DOT. We used the criteria of "Vehicular bridges/Culverts reported to the NBI (>20 ft long)" which makes up about 80% of all bridges included in the assessment, which we deemed a sufficient coverage

## State of Washington

amount for the assertion. We then had Hyung update the qualitative and quantitative parameters we created that we deemed necessary to obtain in order to substantiate a conclusion. These parameters include the inspection date, the primary inspector, whether or not the bridge is included in WSBIS software, and the frequency the bridge is inspected. All of these parameters were not originally included in the bridge assessment report we received. We then calculated the next assessment date of inspection needed to determine if the bridge was assessed within the 24 or 48 month inspection cycle using calendar year end 12/31/23 (since assessments are performed on a calendar year basis) as referenced in the [WSDOT Bridge Inspection Manual](#) to be included in the FY24 ACFR Required Supplementary Information (RSI). We were able to confirm the population was complete on the "Pop. Completeness & Tie Out" tab by comparing the total WSDOT reported bridges with the number of bridges reported to the NBI > 20ft that received a rating. We determined that the population used for sampling had an overall rating of "Fair" or better for 94% of the bridges. To meet the classification assertion, we determined if each bridge's inspection date selected in our sample was within the allotted 24 month inspection cycle to be included in the FY ACFR RSI under the modified approach.

Based on our evaluation of results and sampling risk, we determined the sample provided a reasonable basis for conclusions about the population. We determined bridge inspections were completed as required and support the classification of bridge infrastructure using the modified approach. ***No issues noted.***

### **Pavements:**

#### Substantive tests performed to meet the Valuation & Classification assertion:

Our original test from the risk assessment stated we will "test a sample of highway pavement assessments to determine whether the review is completed to support compliance with the modified approach". DOT's original plan was to include a 2023 percentage in the RSI. This would have been in compliance with their two year cycle of pavement assessments. As the audit progressed we became aware of a data reporting issue. Karen Straus, State Pavement Management Engineer, stated that the most recent data could not be provided due to rating data not being transmitted correctly and was missing. See memo at: [\[2023 GFP Percentage Memo 11-1-2024\]](#). We determined to issue a recommendation related to DOT not being in compliance with their two year cycle of assessments. See issue at: [\[V: DOT RSI Modified Approach: Infrastructure - Pavement\]](#).

Due to this issue OFM elected to report the same percentage as last year. RSI includes the last pavement assessment data which was completed during calendar year 2021. In response to this decision we updated our test in the risk assessment to state "We will rely on the FY2022 State ACFR work performed over highway pavement assessments to determine whether the review is completed to support compliance with the modified approach". We reviewed the FY22 State ACFR audit at: [\[S1Washington-FS22 - H.2.PR - Non Depreciable Assets\]](#). We found that in the FY22 audit we sampled and tested from the calendar year 2021 data and determined the pavement condition assessments are performed by a qualified staff member and assessments collected the necessary data to support the given rating and allow for reporting using the modified approach.

GASB section I.1400.105 notes that assessments must be performed at least every three years. While DOT didn't perform a pavement assessment in 2023 we determined they are still in compliance with GAAP since the last assessment was completed in calendar year 2021. To continue to

## State of Washington

meet the GASB requirement in FY25, they would need to conduct the next assessment by December 31, 2024.

### I.3.PRG - Depreciable Assets (Net of Depreciation)

*Procedure Step:* Summary & Conclusion

*Prepared By:* NJH, 10/17/2024

*Reviewed By:* RKM, 11/19/2024

Purpose/Conclusion:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and*



# State of Washington

*documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

Is information precise enough to catch if misstatements exceeded the tolerable level?

Is information detailed enough to conclude on whether or not there were misstatements?

Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?

How did misstatements occur and how often might they occur again in the population?

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

## State of Washington

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

### **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Understanding of Line Item

*Prepared By:* NJH, 7/2/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the

## State of Washington

significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria:

Record of Work Done:

### **(1) Prior Audit Exceptions:**

None.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

There are two funds that contain depreciable assets for DOT, 410 & 997.

**Fund 410:** A proprietary fund (Transportation Equipment Fund - TEF) is updated whenever equipment is purchased. The Transportation Equipment Fund (TEF) is the primary holder of equipment inventory and financial information related to it. Equipment is purchased and maintained through TEF and then leased to WSDOT for project work. Financial information for this inventory is in FEMS. Capital assets purchased by (or donated to) a Proprietary Fund type remain in the fund, assets purchased by a Governmental Fund type are recorded in the General Capital Asset Subsidiary account (Fund 997).

**Fund 997:** A Governmental fund which includes all other capital assets. The Minor Capital portion of this fund includes all those vehicles and equipment that are purchased directly and not a part of TEF.

We did a break out of the account balances over the prior 2 years for the Net Depreciable Assets at WSDOT as documented at [[Line Item Lead Sheet](#)]. Additionally, a breakdown of the current balances were calculated to determine the composition of the individual general ledger accounts as a percentage of coverage, as documented in the Balance Breakdown tab at [[Line Item Lead Sheet](#)]. We determined we can get adequate testing

## State of Washington

coverage by selection of the following funds GL accounts:

Fund 997, GL 2210, 2220, 2410, & 2420 (Consists mainly of buildings & ferries)

Fund 410, GL 2410 & 2420 (Consists mainly of TEF Equipment)

This accounts for a majority of the total balance of Net Depreciable Assets and was determined to be sufficient coverage for the audit.

### **(3) Updates to Significant Account Matrix:**

None

### **I.3.PRG - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Controls - TEF - TRAINS/FEMS

*Prepared By:* NJH, 7/11/2024

*Reviewed By:* RKM, 8/12/2024

Purpose/Conclusion:

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

#### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.  
In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.

## State of Washington

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

Who or what initiates the control

When (or how often) is the control applied

Who performs the control

As needed, the experience, knowledge and attitude of the person applying the control

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

How the key control is documented or evidenced

## State of Washington

If not obvious from the description, how the control prevents or timely detects and corrects misstatements  
Any exceptions or alternative processing to the normal process  
What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

# State of Washington

Record of Work Done:

## **Material Balance and Assertions**

Internal controls in the TRAINS/FEMS address the following balance:

Depreciable Assets (Net of Depreciation)

For the following assertions:

Existence - There is a risk that capital assets have been replaced, sold or impaired.

Valuation - The amount reported for this line item does not represent actual capitalized costs of assets constructed, purchased, or donated as of the report date.

Valuation - Capital assets are not stated at historical or estimated historical cost.

Valuation - Depreciation may be incorrectly calculated because the wrong asset class code or useful life is entered into the system.

## **Significant Accounting Systems:**

**Fleet Equipment Management System (FEMS)** - Inventory system for fleet equipment and calculating depreciation.

**Transportation Reporting and Accounting and Information System (TRAINS)** - TRAINS is used to post expenditures using Payment Vouchers or Journal Vouchers. TRAINS does not allow the creator to review and approve their own work. All additions, regardless of categorization, get recorded in TRAINS as "transportation expenditures" and then have to be broken out through a reconciling JV. See "*How Transactions are Recorded in AFRS*" section below.

## **Other Systems (Not Significant Systems):**

**Transportation Assets Reporting and Tracking System (TARTS)** – Text file showing value and life-to-date depreciation from capital asset inventory systems.

**COGNOS Datamart and Financial Information Retrieval System (FIRS)** - Read only systems used to access WSDOT accounting system expenditures in the capitalization process.

## **Purchase and Capitalization of Transportation Equipment:**

We met with the following staff on 5/13/24 to discuss the purchase and capitalization of transportation equipment for the Transportation Equipment Fund (TEF):

Jesse Daniels - WSDOT Audit Liaison

Charleen Emmons - Budget and Finance Manager for TEF

Beth De Vaul - AFS Transportation Financial Consultant

Suzi Freeland - Accounting and Reporting Manager



## State of Washington

Below is a discussion on the controls concerning fleet equipment inventory, capitalized asset additions, deletions, and depreciation reported:

Vehicles or equipment are purchased when required through the Transportation Equipment Fund, a non-appropriated, proprietary, internal service fund, budgeted through OFM. Equipment owned in the Fund is rented to only other WSDOT programs, and rent is collected from the programs that are using the vehicle or equipment. Typical vehicles purchased through the fund are road clearing equipment and vehicles for use by DOT personnel. Much of the equipment maintained is heavy equipment with a total 8,552 (as of January 31, 2024- based on TARTS file) items in the depreciable equipment inventory. WSDOT refers to the process of collecting rent revenue and using it to fund TEF operations, including maintenance of equipment through the fund, as a cost recovery program.

Transportation equipment is managed by the agency's Fleet and Equipment Operations, through the Fleet Equipment Management System (FEMS). The equipment's total acquisition costs and depreciation are listed and tracked in FEMS. When a need for equipment is identified, a purchase order must be created after the proper approvals are received by necessary supervisors. All purchase orders are tracked through a spreadsheet and then the information will be updated to the FEMS system once a "tech spec" has been done on the purchase, identifying the proper equipment category. Once the item requested is budgeted and ordered in the system, it will stay in ordered status until it is actually received. The depreciation calculation is an automated process in FEMS once the item is listed in the system with its initial value, expected salvage value at service life end, and service life are entered (**Key Control #1 - Automated Software Calculation - Valuation**). Book value at the end of any month is the capital value less life-to-date depreciation. On a monthly basis, the Budget and Finance Manager, reviews new entries in FEMS (from the prior month) to ensure it is accurate (recorded at cost and donated assets are recorded at their estimated value at time of donation) and reconciles with supporting documentation, such as invoices, work orders, etc. (**Key Control #2 - Valuation**).

The information for service life is from SAAM (Addendum to Schedule A, Subsection [30.50.10.b](#)) except where DOT experience has shown that a different service life is indicated. For those pieces of equipment DOT requests written approval from Office of Financial Management (OFM) to document the change in depreciation due to change in service life.

Equipment expenditures are capitalized based upon the procedures in Section 2-5 Capital Assets and Inventories in WSDOT Accounting Manual M 13-82 and [SAAM 30.20.20](#). According to SAAM, equipment expenditures are a capital asset if there is a unit cost (including ancillary costs) of \$5,000 or greater. WSDOT in general capitalizes extraordinary repairs, betterments, or improvements that increase the future benefits of an existing asset by extending its useful life, increasing the capacity or efficiency, or providing a substantial improvement in the quality of output or a reduction in operating costs. Betterments are not added to a vehicle's value until the betterment is installed. Once a betterment is installed to a vehicle, the value will be updated in FEMS.

The actual existence of the vehicles and equipment is verified with a complete physical inventory performed every other year (**Key Control #3 - Existence**). The inventory verification process is required to be complete by June 30 every other year and requires pictures to be attached as part of the inventory process. Vehicle use can also be monitored through review of fuel card usage, since the cards are specific to each vehicle.

## State of Washington

When items are identified for disposal due to overuse (too many miles or hours), obsolescence, or past their scheduled life span, they are disposed of through procedures defined in [SAAM 30.40.45](#) and other related regulations and are sold as a surplus through the Department of Enterprise Services (DES).

### Monthly Review and Transfer of Data to Headquarters

Each month after the close of the month for TRAINS, FEMS provides a report of all units that are capitalized for depreciation. This process occurs after the end of the month, usually in the second week of the month to allow all areas to report. Each unit is identified by number and the monthly depreciation amount is included. These reports are divided by the region they are part of six total regions and Headquarters.

The Budget Finance Manager reviews the monthly fixed asset and depreciation calculations and reports for vehicles and equipment inventoried in FEMS. They first check to make sure that the report is different from the previous month. Their expectation is there will be differences due not only to the fact that it would be a different month but also that the automatic depreciation amount in FEMS will be calculated with a full month of depreciation for any new equipment purchased or donated during the month. The Budget Finance Manager also looks for units that show \$0 depreciation for the month to research and address later in the monthly depreciation reconciliation process. They also review the disposal report from FEMS to make sure that all the disposed equipment is properly identified and valued.

After the report is reviewed and determined to be reasonable, it is released as a detailed flat file from FEMS, to the Transportation Financial Consultant and TARTS, with a summary total amount to TRAINS where it sits in transit until released. While in transit, TRAINS compares the flat file to the depreciation that is calculated by FEMS and produces an error report that shows all items with differences which is also sent back to the Budget Finance Manager. The Assistant Budget Finance Manager looks in TRAINS to ensure the depreciation documents from the FEMS interface to TRAINS are accepted. Then they go through a depreciation reconciliation process that uses the previous month's TARTS file, current month's TARTS file, equipment number change file, equipment disposal file, FEMS depreciation by unit file, and TRAINS depreciation amounts from COGNOS. This identifies depreciation by equipment number between TRAINS and FEMS. This also identifies units disposed, unit number changes, and units where the FEMS and TRAINS depreciation amounts do not match. The Assistant Budget Finance Manager (or Budget Finance Manager) verifies the items were indeed put into service on the dates listed and recalculates the adjustment made by FEMS to verify that amount. Any further adjustments needed are determined by the Assistant Budget Finance Manager (or Budget Finance Manager), who prepares the adjusting JV for TRAINS every month, which are reviewed and signed by the Transportation Financial Consultant or the Accounting and Reporting Manager of the Accounting and Financial Services (AFS) division. The Transportation Financial Consultant completes any JV necessary for AFRS adjustments, which are reviewed by the Accounting & Reporting Manager or Assistant Manager and then releases the JV in TRAINS (from the adjusted original summary total from FEMS) which is picked up in the nightly upload to AFRS.

### **How Transactions are Recorded in AFRS:**

The Transportation Financial Consultant (Beth De Vault) updates the fund equity amounts in TRAINS and AFRS using the various inventory system reports and the monthly TARTS reports to create an Excel workbook that compares the current quarters asset reporting to the previous quarter's asset reporting and on a quarterly basis through electronic journal vouchers that are entered separately in TRAINS and AFRS. TRAINS

## State of Washington

automatically records all expenditures in AFRS as transportation expenditures. These are recorded in AFRS via nightly upload. At the end of each quarter, the Transportation Financial Consultant (Beth De Vault) prepares a JV to adjust the transportation expenditure balance for the amounts that should be recorded as TEF. Then, the Accounting and Reporting unit performs monthly TRAINS/AFRS fund and GL reconciliations to ensure transactions are properly reported within AFRS. **(Key Control #4 - AFRS: Valuation - Manual)**.

One of the following staff members in the Accounting and Reporting section reviews the electronic journal voucher workbooks and releases the journal vouchers: The Accounting and Reporting Manager, or the Accounting & Reporting Assistant Manager. The person writing the JV cannot be the reviewer/releaser.

The purpose of the above procedures is to ensure the data that is entered into TARTS to be picked up by TRAINS on a daily interface is accurate and complete so that when TRAINS and AFRS interface on a nightly basis the information update transferred to AFRS is accurate and complete.

### Key Controls are as Follows:

**Key Control 1 - Automated Software Calculation - Valuation:** Deprecation is automatically calculated for new additions once listed in FEMS and its initial value, expected salvage value at service life end and service life are entered.

**Key Control 2 - Valuation:** Each month, the Budget Finance Manager reviews new entries in FEMS to ensure newly added assets are recorded at their cost. The Budget Finance Manager reconciles monthly depreciation between FEMS and TRAINS to ensure that both systems match.

**Key Control 3 - Existence:** A physical inventory is performed every other year to ensure that recorded assets actually exist.

**Key Control 4 - Valuation:** The Accounting and Reporting unit performs monthly TRAINS/AFRS fund and GL reconciliations to ensure transactions are properly reported within AFRS.

### Noted Weaknesses are as Follows:

None

### I.3.PRQ - Depreciable Assets (Net of Depreciation)

*Procedure Step:* Key Control #1 (Automated)

*Prepared By:* NJH, 8/26/2024

*Reviewed By:* RKM, 8/27/2024

# State of Washington

## Purpose/Conclusion:

**Purpose:** To confirm whether depreciation is automatically calculated for new additions once listed in FEMS and its initial value, expected salvage value at service life end and service life are entered for **Key Control #1 for TEF - TRAINS/FEMS** in order to assess control risk.

**Conclusion:**

Based on our test results, we concluded that the automated control **was** in place. General controls related to the automated control **were not** tested, therefore, we assess control risk at MAX.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - TEF - TRAINS/FEMS\]](#).

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

# State of Washington

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other*

## State of Washington

*calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

# State of Washington

## **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented

# State of Washington

in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

## **Manual vs. Automated Interfaces**

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.



## State of Washington

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered “manual” since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient’s age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient’s name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or

## State of Washington

may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

- Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

- Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

# State of Washington

## Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control #1 (Automated Software Calculation - Valuation):** Deprecation is automatically calculated for new additions once listed in FEMS and its initial value, expected salvage value at service life end and service life are entered.

## **STEP 1: Understand Automated Key Control**

The understanding for this system is documented above in the [[Controls - TEF - TRAINS/FEMS](#)] step.

## **STEP 2: Confirm and Test Automated Key Control:**

We confirmed the key automated control as follows, to determine whether the software calculation correctly valued each transaction:

We obtained a copy of an example of the FEMS interface [[FEMS Unit Category Example](#)] for where the user manually inputs the necessary parameters pertaining to the specific TEF asset. We also obtained a copy of the depreciation parameter's [[FEMS Depreciation Parameters](#)] which gives the user an understanding of the necessary input fields required in FEMS such as the term, salvage %, and the type of asset. Additionally,

## State of Washington

the user relies on outside authoritative literature for the service life input into FEMS from guidance listed in SAAM (Addendum to Schedule A, Subsection [30.50.10.b](#)).

To confirm the automated control we re-performed the depreciation calculation for asset number 10A04303 (2023 Ford Mach E purchased on 12/19/2023). See re-calculation at [[TEF Automated Key Control #1 Testing](#)]. Asset information was provided by Charleen Emmons, Budget & Financial Manager, on 6/14/24 after a request for a random new asset addition for FY24. Note that because DOT selected the asset for us to evaluate and we did not randomly select it ourselves it could be subject to some level of bias risk for this control. However, given the longstanding integrity and professionalism of the DOT staff we don't consider this an issue. Recalculations were made to confirm monthly depreciation amount and LTD depreciation. The correct useful life was determined based off of "TEF Schedule of Useful Lives" which is submitted to OFM (See: [[TEF Schedule of Useful Lives Fiscal Year 2024 \(PBC\)](#)] ). Salvage value, salvage value %, and LTD Depreciation were supplied by the file *01C08003 Unit Accounting Frame from FEMS.png* provided by Charleen Emmons. Recalculation matched FEMS amount with the only difference due to rounding.  
**No issues noted.**

### **STEP 3: Understand General IT Controls**

#### FEMS General IT Controls:

We met with the following DOT staff on 5/29/24 to gain an understanding of general IT controls of the FEMS system:

Charleen Emmons - TEF Budget and Finance Manager

Dan Butler - TEF Database Administrator

Jesse Daniels - WSDOT Audit Liaison

FEMS is the system that automatically calculates depreciation for the Transportation Equipment Fund (TEF). The automatic depreciation calculation uses the service life (term), expected salvage value (entered as a percentage in FEMS), and unit cost.

There have not been any changes to the depreciation calculation since the system was purchased. The actual calculation itself is set by the system and was purchased with the system already having the depreciation calculations. Charleen and Dan have never experienced an error in the depreciation calculations. The system uses the parameters [[FEMS Depreciation Parameters](#)] for a unit category to calculate depreciation. The only way the depreciation could be wrong would be if the parameters were wrong, which are manually entered into the system.

A unit is an item purchased and entered into the system, such as a truck. Each unit is assigned to a unit category [[FEMS Unit Category Example](#)], through a "tech spec". The unit category is already in the system, along with the unit information used to automatically calculate depreciation. The unit category is set up through a process that goes through headquarters. Charleen is usually the person who will create or request a new unit category with the unit information and parameters, then it is reviewed by Asset Management. Access is limited to set up a new unit category. There is a memorandum that is sent out if there is a new unit category in the system. When a unit is assigned a unit category through the tech spec, it is never actually added to the category until Dan or Charleen review and accept it to the category. Regions can view the unit category their unit was assigned to through the tech spec, which contains the parameters, but they cannot change it or the parameters. If the region feels the tech spec was incorrect, they have to request to headquarters to change the tech spec. Changing the tech spec would give the item a new

## State of Washington

unit category, which would change the depreciation parameters for that unit. The actual parameters, such as salvage percentage or service life, would not be changed for that unit category if the tech spec was changed, the item would just be given a different unit category.

On certain occasions, it could be identified that parameters, such as life cycle or salvage value, need to be changed. Access is limited to change parameters, but Charleen or someone else with access at headquarters could change those parameters for the unit category. **There is an access list and a process for changing parameters (Key General IT Control).** For depreciation to be changed, the parameters for a unit category would have to be changed, the actual calculation itself could not be changed. The calculation and the parameters used in the calculation are set by the system and have never been changed. The only way a unit could depreciate wrong would be if the wrong unit category was assigned during the tech spec, and that is a manual process, so the system could not depreciate the unit category incorrectly. Betterments may cause depreciation of a unit to change. Betterments are added to a unit and it increases the value of the unit. As documented above in the understanding of TEF, new entries into FEMS are reviewed monthly to ensure that the information, unit category, and entry is accurate.

### **STEP 4: Confirm Key General IT Control:**

**Key General IT Control:** There is an access list and a process for changing parameters.

To confirm this general IT control, we met with Dan Butler, TEF Database Admin, and Charleen Emmons, TEFS Budget and Finance Manager, to observe a walkthrough of the FEMS system access. Dan shared with us that on the FEMS interface front end that there are different frame groups that certain users have access to. He shared his screen and showed us the highest level of access, which is a role called "HQ System Admin". We were able to view that there were seven users currently at DOT who have access at this level. Three of these are IT related non-users (Python script user and IT database/network group). The other few were Dan, Charleen, & each of their respective managers. Dan showed us how by accessing the "Role Maintenance" frame group (which only the HQ System Admin have access to) he is able to make changes to assigned roles and which roles/groups have what permissions. There are three permissions we saw within this frame; "Read, Update, & Full Access". Dan noted that each role or group of staff has certain permissions assigned to the necessary fields that could be modified on the FEMS Main Menu page as it relates to an asset. He verified this by logging into a "fake" account with TEF technician level parameters and showed how all of the input fields on a particular asset were grayed out / un-editable. ***No issues noted.***

We inquired with Dan about bad actors who might already have access as the HQ System Admin role. He noted here that there is nothing in place from another HQ System Admin from removing another HQ System Admin other than keeping the actual quantity of users with that role to a minimum. Dan stated that this role is not merely given based on position within TEF but rather on the actual duties they are responsible for performing, even if on occasion. During our meeting, Dan navigated to a section within role maintenance called the "Table Column Audit" section. This allows HQ System Admin to turn on logged traces of what changes were made to certain parameter fields within FEMS. This data is stored and backed up on a server. This has not been in place until this meeting when Dan turned them all on, stating that it would be a good security and accountability check to have in place and was unsure as to why it was not turned on or used. ***No issues noted.***

### **STEP 5: Test Key General IT Controls:**

## State of Washington

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### I.3.PRG - Depreciable Assets (Net of Depreciation)

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* NJH, 6/20/2024

*Reviewed By:* SHW, 7/2/2024

Purpose/Conclusion:

**Purpose:**

To confirm whether the Budget Finance Manager reviews new entries in FEMS to ensure newly added assets are recorded at their cost and reconciles monthly depreciation between FEMS and TRAINS (key control #1 for TEF - TRAINS/FEMS) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation.*

## State of Washington

*Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

## State of Washington

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #2 (Valuation):** Each month, the Budget Finance Manager reviews new entries in FEMS to ensure newly added assets are recorded at their cost. The Budget Finance Manager reconciles monthly depreciation between FEMS and TRAINS to ensure that both systems match.

The understanding for this system is documented above in the [\[Controls - TEF - TRAINS/FEMS\]](#) step.



# State of Washington

## **1. Confirmation of Key Manual Control:**

Charleen Emmons, TEFS Budget and Finance Manager, provided us with the FEMS/TRAINS Monthly Depreciation Comparison for April 2024. This report is taken from the TRAINS Access data workbook that provides depreciation amounts from both FEMS and TRAINS. That data is entered into a pivot table which compares any differences that arise for depreciation between TRAINS and FEMS. If amounts match between systems, the difference will show zero or 0.01 (due to rounding). Any amounts greater are reviewed by Charleen. We reviewed the data from the TRAINS Access data workbook and found that it had tabs for previous month and current month TARTS data, units changed, sold/disposed units, and unit depreciation from TRAINS. This information flowed accurately to the FEMS & TRAINS Monthly Depreciation file where TRAINS and FEMS depreciation were compared. There were 4 instances where differences were shown. Per the comments in the file, each instance was due to either TRAINS only being sent partial depreciation or "Research - part of sold". The total difference for the month was \$1,170. A JV will be used to increase depreciation expense in TRAINS for the partial amounts that were missed. We found that depreciation recorded in FEMS was reconciled to TRAINS data and differences were adjusted correctly. *No issues noted.*

We reviewed invoice 3PU413 for unit 01C08003. We found that the initial purchase price for the unit was \$62,844 from Bud Clary Ford Hyundai, which matched to FEMS as well as the acquisition date of 12/19/23. We found that the unit was recorded in FEMS accurately based on historical value and additions. *No issues noted.*

### **Noted Weaknesses are as follows:**

**None**

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Key Control #3 (Manual)

*Prepared By:* NJH, 7/1/2024

# State of Washington

Reviewed By: SHW, 7/2/2024

Purpose/Conclusion:

**Purpose:**

To confirm whether a physical inventory is performed every other year to ensure that recorded assets actually exist for **Key Control #3 for TEF - TRAINS/FEMS** in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated"*

## State of Washington

*step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider

## State of Washington

*whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*

*B. Controls are not related to a "significant risk" identified in the audit plan.*

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #3 (Existence):** A physical inventory is performed every other year to ensure that recorded assets actually exist.

The understanding for this system is documented above in the Controls - TEF - TRAINS/FEMS step.

### **1. Confirmation of Key Manual Control:**

We received and reviewed the physical inventory of assets performed every two years (each biennium). The last physical inventory was completed during FY2024. DOT TEF assets are divided among 9 different regions/programs as follows:

Northwest Region (NWR) - completed 6/25/24

North Central Region (NCR) - completed 6/25/24

Olympic Region (OR) - completed 6/21/24

Southwest Region (SWR) - 6/28/24

South Central Region (SCR) - completed 6/4/24

Eastern Region (ER) - completed 6/26/24

Materials Laboratory Region (MatLab) - completed 6/24/24

# State of Washington

GeoMetrix Region - (GS) - completed 2/22/24  
Printing Services Region (RP) - completed 2/21/24

Charleen Emmons, TEF Budget and Finance Manager, provided us with the portion of the TEF Operation Manual pertaining to Inventories (Chapter 12). The manual states that inventory lists are to be created by HQ TEF and will be provided electronically to each region/program prior to the due date for completion of the inventory. Once the physical inventory has been performed, the inventory control officer for each region/program will send a letter of inventory completion to the TEF fleet administrator.

We received the inventory completion letters from all nine regions/programs from Charleen Emmons. We reviewed the letters provided and noted inventories were stated as being completed and signed by the region's Inventory Control Officer. We determined Department biannual inventory and supervisory review of inventory processes and results provides assurance of existence of depreciable assets. ***No issues noted.***

## **Noted Weaknesses are as follows:**

**None**

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.3.PRQ - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Controls - Buildings - TRAINS/CAFM

*Prepared By:* NJH, 6/20/2024

*Reviewed By:* RKM, 7/1/2024

Purpose/Conclusion:

## **Purpose:**

# State of Washington

To gain an understanding of internal controls.

## **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

## **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

## State of Washington

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- Initiation:* How are transactions initiated?
- Authorization:* How are transactions and accounting record maintenance authorized?
- Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

# State of Washington

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Material Balance and Assertions**

Internal controls in the TRAINS/CAFM address the following balance:

Depreciable Assets (Net of Depreciation)

For the following assertions:

Existence - The furnishings, equipment and capitalized costs have been disposed, replaced or otherwise impaired.

Valuation - The amount reported for this line item does not represent actual capitalized costs of furnishings and equipment constructed, purchased, or donated as of the report date.

Valuation - Newly added furnishings and equipment are not stated at historical or estimated historical cost.

Valuation - Depreciation may be incorrectly calculated because the wrong asset class code or useful life is entered into the system.

Significant Accounting Systems:

**Computer Aided Facilities Management System (CAFM)** - WSDOT’s system of record for the inventory of all owned and leased buildings and capitalized improvements. CAFM automatically calculates straight-line depreciation based on the asset's cost and useful life.

**Transportation Reporting and Accounting and Information System (TRAINS)** - TRAINS is used to post expenditures using Payment Vouchers or Journal Vouchers. TRAINS does not allow the creator to review and approve their own work. All additions,



## State of Washington

regardless of categorization, get recorded in TRAINS as "transportation expenditures" and then have to be broken out through a reconciling JV. See "*How Transactions are Recorded in AFRS*" section below.

### Other Systems (Not Significant Systems):

**Transportation Assets Reporting and Tracking System (TARTS)** – Text file showing value and life-to-date depreciation from capital asset inventory systems.

We met with the following staff on 5/29/24 to gain an understanding of controls for the capitalization of buildings/structures:

Jesse Daniels - WSDOT Audit Liaison

Krystle Mize - Capital Facilities Budget and Financial Manager

Stephanie Alexander-Butters - Capital Facilities Assistant Program Manager

Suzi Freelund - AFS Accounting and Reporting Manager

There are currently 618 capitalized structures with a total capital cost of \$364,345,156. As with all capitalized assets at WSDOT outside of Infrastructure Assets, which use the [GASB 34](#) Modified Approach, the depreciation method is straight-line depreciation. Depreciation amounts are based on the useful life schedule and commodity codes as listed in [SAAM 30.50.10](#). The facilities on the report have a commodity code of 0535, 0550, 5410 or 0655.

Facilities with a 0535 Commodity Codes are Public Restroom and have a useful life of 35 years.

Facilities with a 0550 Commodity Code are buildings and have a useful life of 50 years.

Facilities with a 5410 Commodity Code are prefabricated or portable structures and have a useful life of 50 years.

Facilities with a 0655 Commodity Code are improvements other than buildings and have a useful life of 25 years.

Buildings, building improvements, and leasehold improvements with a cost of \$100,000 or greater are considered as fixed assets. The cost of the improvements can be considerably less than that amount, it is the total value of the structure that needs to be more than \$100,000 (per [SAAM 30.20.20](#)). If the building improvements capitalized are less than 10% of the total value of the building, the improvement will not be depreciated separately. If the improvement increases the value of the building or if there is an increase in the probable life of the building, that is reviewed by the Budget Analyst to determine if there is need to change the depreciation. If any of those occur, then CAFM will be updated.

### Capitalization of Buildings/Structures

When buildings or other structures that are not intended to be part of the non-depreciable infrastructure of WSDOT are proposed, a work order is developed by the Capital Facilities management. Once the work order is complete (construction completed and structure in use), the Capital Facilities team will review the work order for completeness and approval for capitalization (**Key Control #1 - Existence**). Quarterly, they provide a list of completed work orders to the Capital Facilities Budget and Financial Manager's team, where they will check to ensure all information and detail for the work is provided. When there is enough information, they can determine whether something needs to be

## State of Washington

capitalized. A Capitalization Form is filled out and submitted to the Facilities Inventory Specialist for entering data into CAFM for capitalization and depreciation. CAFM is WSDOT's computerized system of record for used by the facilities office to inventory all WSDOT owned and leased buildings and associated capitalized improvements. The useful life is based on the OFM commodity code list ([SAAM 30.50.20](#)). CAFM automatically calculates straight-line depreciation based on the asset's cost and useful life (**Key Control #2 - Automated: Valuation**).

After the depreciation amounts calculated in CAFM are reviewed and reconciled by the Transportation Financial Consultant, Beth De Vul, the report is then reviewed by the Accounting and Reporting Manager, Suzi Freeland, who performs a final review for accuracy and reasonableness. Beth reviews the CAFM listing to ensure that assets recorded are properly valued and depreciated correctly. Suzi Freeland or Beth De Vul then pulls the data from CAFM to TARTS to perform a reconciliation of CAFM vs. TARTS to verify that the historical cost and accumulated depreciation from CAFM agree with data pulled to TARTS (**Key Control #3 - Valuation**). TARTS pulls data from all inventory systems, including CAFM, so a review between TARTS and TRAINS can be done for all inventory systems by Beth using a TARTS vs. TRAINS reconciliation.

### **How Transactions are Recorded in AFRS:**

Depreciation is given to the Transportation Financial Consultant (Beth De Vul) in the form of several reports. Capital Facilities provides a report for capitalized structures from CAFM. The Transportation Financial Consultant uses the Capital Facilities report and on a quarterly basis enters the depreciation amounts into TRAINS, then creates TRAINS and AFRS journal vouchers to record the increase or decrease in asset balances and depreciation in both financial systems. The Accounting and Reporting Manager reviews the documentation and calculated amounts then releases the journal vouchers in the system they were recorded in. TRAINS automatically records all expenditures in AFRS as transportation expenditures. These are recorded in AFRS via nightly upload. At the end of each quarter, the Transportation Financial Consultant (Beth De Vul) prepares a JV to adjust the transportation expenditure balance for the amounts that should be recorded as buildings. Then, the Accounting and Reporting unit performs monthly TRAINS/AFRS fund and GL reconciliations to ensure transactions are properly reported within AFRS (**Key Control #4 - Valuation**).

### **Key Controls are as Follows:**

**Key Control 1 - Existence:** When buildings or other structures that are not intended to be part of the non-depreciable infrastructure of WSDOT are proposed, a work order is developed by the Capital Facilities management. Once the work order is complete (construction completed and structure in use), the Capital Facilities team will review the work order for completeness and approval for capitalization and input into CAFM.

**Key Control 2 - Automated - Valuation:** CAFM system automatically calculates straight-line depreciation based on the asset's cost and useful life.

**Key Control 3 - Valuation:** The Financial Consultant at WSDOT's headquarters' Accounting and Finance Division prepares the Inventory Systems vs. TARTS Analysis to verify the Capital Facilities historical cost and accumulated depreciation from Facility Inventory Division (CAFM) agrees with the data shown in TARTS.

## State of Washington

**Key Control 4 - Valuation:** The Accounting and Reporting unit performs monthly TRAINS/AFRS fund and GL reconciliations to ensure transactions are properly reported within AFRS.

### Noted Weaknesses are as Follows:

None

### I.3.PRG - Depreciable Assets (Net of Depreciation)

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* NJH, 8/28/2024

*Reviewed By:* RKM, 8/28/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm whether buildings or other structures that are not intended to be part of the non-depreciable infrastructure of WSDOT are proposed, a work order is developed by the Capital Facilities management. Once the work order is complete (construction completed and structure in use), the Capital Facilities team will review the work order for completeness and approval for capitalization and input into CAFM for **Key Control #1 for Buildings - TRAINS/CAFM** in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented*

## State of Washington

*key controls).*

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

**Key Control #1 (Existence):** When buildings or other structures that are not intended to be part of the non-depreciable infrastructure of WSDOT are proposed, a work order is developed by the Capital Facilities management. Once the work order is complete (construction completed and structure in use), the Capital Facilities team will review the work order for completeness and approval for capitalization and input into CAFM.

The understanding for this system is documented above in the [\[Controls - Buildings - TRAINS/CAFM\]](#) step.

## **1. Confirmation of Key Manual Control:**

To confirm this key control, we received a walkthrough on 7/17/24 with Krystle Mize (Capital Facilities Financial Manager), Stephanie Alexander-Butters (Capital Facilities Assistant Program Manager), and Elena Fehr (Facilities Inventory Specialist) as well as inspected relevant documents that we acquired on 6/11/24 from Jesse Daniels, Audit Liaison, on behalf of Krystle Mize. We chose to evaluate the capital asset "Dayton Ave Annex Building" which we inquired about and documented additional ROWD pertaining to another key control at [\[Key Control #2 \(Automated\)\]](#). We inspected the document *Project Capitalization Form* to determine if the asset was listed to be eventually input into CAFM as well as the relevant costs making up that asset. The Dayton Annex Building is comprised of two identifiable costs shown on this sheet, \$1,799,132 from work order #00932 and \$15,390 from work order #PO1100 for a total asset cost of \$1,814,522. From this inspection we inquired about the two relevant work orders during our walkthrough to confirm the work order exists for this asset. Stephanie Butters shared with us a live view of the original #00932 work order, but had us note that there are 52 work orders with that number to include various additions and project changes. She explained that this project comes out of a certain fund within DOT fund management and all updates/changes are ran through that fund until they reach the budgeted funding amount. The additional \$15,390 was a change order later in the construction process, on 4/11/23, beyond the budgeted amount for the fund, so it came out of DOT facilities operating change fund, hence the different work order PO1100 which she shared with us during our walkthrough. Krystle pulled up a copy of the original contract work details by the contractor showing a breakdown of all of the costs that make up the Dayton Ave site overall (which included the Dayton Annex Building). On this sheet we could identify the majority of the original costs as well as the addition for the Annex Building. After confirming the necessary work orders existed and the proper amounts matched what was on the capitalization form, we had Elena Fehr show us a live view of the CAFM system for the Dayton Annex Building with a cost basis of \$1,814,522, showing no variances. From our walkthrough and inspection of documents we can confirm that the Annex Building exists and that the key control is in place and operating effectively. ***No issues noted.***

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be

## State of Washington

effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Key Control #2 (Automated)

*Prepared By:* NJH, 8/28/2024

*Reviewed By:* RKM, 8/28/2024

#### **Purpose/Conclusion:**

**Purpose:** To determine whether CAFM system automatically calculates straight-line depreciation based on the asset's cost and useful life (**Key Control #2 - Buildings - TRAINS/CAFM**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively. However, we identified an error in a manual process that caused a misstatement in the automated depreciation calculation. See: [\[E: WSDOT Depreciable Assets Manual Input Error\]](#).

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Controls - Buildings - TRAINS/CAFM\]](#).

We noted **the following** weaknesses or deficiencies in internal controls:

**The manual error of not properly updating the "date acquired" field and/or the "date placed in service" field in CAFM caused an incorrect depreciation calculation.**

#### **Testing Strategy:**

# State of Washington

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.



## State of Washington

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

# State of Washington

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

## **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

## **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

# State of Washington

## **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Information Technology](#) Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This

## State of Washington

process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

## State of Washington

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

## State of Washington

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An "**electronic signature**" can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A "**digital signature**" is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the**

# State of Washington

**Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

**This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control #2 (Valuation):** CAFM system automatically calculates straight-line depreciation based on the asset's cost and useful life.

**STEP 1: Understand Automated Key Control:**

The understanding for this system is documented above in the [\[Controls - Buildings - TRAINS/CAFM\]](#) step.

**STEP 2: Confirm and Test Automated Key Control:**

On 6/11/24 we received an email correspondence from Jesse Daniels, Audit Liaison, forwarded on behalf of Krystle Mize, DOT Budget & Financial Manager, that noted the following attestation: "We did not add a **new** FY24 asset that meet the threshold for capitalization so we cannot provide an example of depreciation calculated for a new FY24 asset, supporting documentation making up the asset's cost or the capitalization form." We determined that the next most useful confirmation of this key control would be to obtain an understating of the process of a new asset placed in service (PIS) for FY23 as that is the most recent year with capital additions/improvements that met the capitalization threshold. **No issues noted.**

Krystle Mize provided us with a copy of several relevant documents on 6/13/24 pertaining to the FY23 addition of a capital asset "Dayton Ave Annex – 1017BM07" where she noted that there were two additions during this project for the main building & annex building. These documents include:

1017BM07 – 2024-06-10: *This is the form submitted from Facilities Inventory Specialist (Elena) for the annex building depreciation.*

Dayton Capitalization: *Capitalization form submitted to Facilities Inventory Specialist (Elena) by Budget & Financial Manager*

v3 Project Capitalization Form: *Supporting documents for calculations.*

Pay App #38: *Supporting documents for calculations. Amounts that tie to the Annex Building are lines referenced "Exterior Shed Building" on page 12 & 13. Additionally, on page 19, please see "PCCO # 57 COP161 – Annex Motor Operated Doors"*

To confirm this automated control we preformed analytical procedures to re-calculate the CAFM depreciation of this asset at [\[SAO CAFM Recalculation - Dayton Annex\]](#) based on the supporting documents provided to us as well as our knowledge from a CAFM IT walkthrough on 6/5/24. We chose to evaluate the annex building which was placed in service on 11/18/21. We determined that the asset's useful life of 50yrs (600mo.) was classified correctly by referencing [SAAM 30.50.20](#) with code 0550 referenced in the spreadsheet. **No issues noted.**

We performed two different calculations to confirm this control on the sheet titled "SAO Calc". The first was to determine if the stated/calculated

## State of Washington

number of depreciation periods elapsed matched with our recalculation by backing into the depreciation periods using the life and depreciation per period. Our second calculation was a figure check for the cost, A/D, current value, and monthly depreciation compared to our recalculated figures. From these two calculations we noted two mathematical issues that arose: the first being a slight \$25 difference in the monthly depreciation amount (FEMS was about \$25 more than it should have been) and the second issue being a \$14,877 difference in total A/D which we calculated to be about 5 months of missing depreciation.

We met with Krystle & Elena on 6/27/24 to address these issues and try to gain a better understanding of what had happened to cause these errors. Elena noted that she had forgot to change the actual depreciation start date in another database table. Elena made that change and then sent us back a revised copy of the CAFM calculation table and we were able to run the same tests described above, see "DOT Corrected" sheet. The corrected error shows a total difference of \$123 in A/D which we can attribute to rounding over time and is determined to be insignificant. The other corrected error was the monthly depreciation to the correct amount \$3,024. We inquired with Elena about how this amount was changed (manual or automatic) and determined that the straight line calculation is an automated, un-editable parameter in CAFM. She stated that the system uses a logical formula based on the date acquired and date placed in service to determine the monthly depreciation amount. In the uncorrected date acquired field, the CAFM system calculated monthly depreciation for 595 months instead of the full 600 months. Once the date acquired field was updated and corrected, the CAFM system automatically calculated the correct monthly depreciation of \$3,024.

**The manual error of not properly updating the "date acquired" field and/or the "date placed in service" field in CAFM will be addressed as a verbal issue. See: [E: WSDOT\_Depreciable Assets Manual Input Error].**

### **STEP 3: Understand General IT Controls:**

The understanding of the general IT Controls is documented below from our inquiry about the CAFM system with Richard Daniels, GISP - DOT Technology Services Division, where he explained the following:

The CAFM system consists of thick clients known as Archibus and Smart Client that are currently only used for Admin tasks, a modern Web application known as WebCentral, and the shared SQL Database known as CAFM. Throughout the history of CAFM at WSDOT multiple web applications have been used against the CAFM database, those included CSMM, FM Studio, Infrastructure.Net, and now WebCentral. The web application is a configured commercial off the shelf (COTS) product. The code base is Vendor supported and human readable. The code consists of view files and java and JavaScript compiled coded that run under a TomCat web server environment. WSDOT maintains a complete database side environment with Development, Quality Assurance, and Production SQL Servers. On the web application side WSDOT has a Development, QA and Production project environment as well. All code or system level data changes are tested in the DEV and QA environments before being promoted to production.

Code changes within the application are done at the Vendors internal testing site then provide to WSDOT via SFTP for loading into our Development and QA environment on ARCHIBUS (wsdot.loc) (<http://hqpolymappcmms1p.wsdot.loc:8084/archibus/>) for final testing and acceptance. Accepted code changes are moved to the production server using a managed repliweb process that copies 'changed' files to the



## State of Washington

production server. This enables support staff to move code without directly accessing the production server. Server support and one Vendor support person have remote login permissions on the production application server. **In practice, only Richard Daniels and Elena Fehr, Facilities Inventory Specialist, and Brian Branners from Facilities, have permissions to edit code on the DEV/QA web server (Key General IT Control).**

Database structure changes are done using internal tools contained within the WebCentral and SmartClient application. This is made possible by the presence of a 'Fields' and 'Tables' table in the database that when used together, provide the definition of all tables and views contained within the database. When the "Rebuild" table structure command is issued from the WebCentral or SmartClient application the specified table will be rebuilt from scratch based on the table definition, data within the table is retained and copied into the newly created table (i.e., the old table is backed up prior to executing the drop and create SQL statements required by the "Rebuild" command).

Separate from the database structure within the SQL database itself are stored procedures, triggers, and SQL Agent Jobs. The stored procedures are used in four main roles, (1) populated drop downs within the application, (2) provide formatted data for reports, and (3) support ETL interfaces, and (4) triggered on demand to execute a specific calculation (e.g., issue work orders request based on preventive maintenance schedules). The SQL Agent jobs execute stored procedures at a give date time to support interfaces and internal. Anyone with update or DBA level access to the database could make changes to the data, executed these procedures, or alter a table structure; however, on the (re)deployment of the database structure from SmartClient, any database structure changes made directly within SQL would be reverted. To prevent data loss the Production data is backup daily and retained for over 6 months.

In the Production SQL database the only individuals who could change the data directly (vs. with DevOps) are the web application special user (account that talks between the web application and the database), WSDOT SQL Database Administrators, and CAFM App support team members. The list would include members of Data Based Administrators of the TSD Data Resource Management Office and Richard Daniels and Hazim Mohaisen from the TSD Solutions Development & Modernization Team and Elena Fehr, Brian Branners from Facilities. Permissions in Production for the database structured and stored procedures are strict (view only). This was done to force users to use the built in methods provided by WebCentral and SmartClient to deploy database structure changes.

### **STEP 4: Confirm Key General IT Controls:**

**Key General IT Control: In practice, only Richard Daniels, and Elena Fehr, Facilities Inventory Specialist, and Brian Branners from Facilities, have permissions to edit code on the DEV/QA web server.**

To confirm the general IT control met with Richard Daniels, GISP - DOT Technology Services Division, on 7/9/24 to observe a walkthrough and inquire of the control. Richard shared his screen and walked us through the login process for Web Central, where the Archibus application is which is used by the CAFM Database Server. He showed what happens when a user not authorized by the system tries to login, which results in an error pop up saying the password or user name is wrong. He shared with us that the user name can specialized (for certain development teams) or simply just the DOT 8 digit user ID that employees have. For passwords, Richard shared that these are not the same passwords used in admin in

## State of Washington

the active directory, but are specially created passwords. Richard informed us that all user permissions and parameter's for granting access are done at the DOT Network level. Once into the Archibus system, Richard showed us the user access list to CAFM & Archibus. Only 14 people have access at all (consisting of IT, Facilities staff, & vendor personnel) and only 6 have the highest level of admin capabilities (for creating and removing users). Of these 6, there are 2 IT personnel and 4 facilities personnel. Richard explained the following order of necessary requirements in order to access or make changes in the CAFM system front end DEV environment:

1. Obtain a DOT Credential to use the DOT Intranet
2. Obtain/know the web server hosting alias
3. Have an Archibus/Web Central Account (that meets password requirements)
4. The account has to have certain "edit/modify" permissions only granted by super-user admin in order to make changes.

For back end DEV and SQL Database changes, all access levels and permissions are granted/created by TES STAR Team or the Network Admin, both of which are separate divisions under DOT's Technology Service Department (TSD). Richard walked us through virtually logging into the SQL DEV Database for CAFM. Richard noted that every year the IT team will pull a list from CAFM database of users and validate users with current DOT email's to ensure that anyone who has access (at any level) to make changes to the CAFM system are current employees at DOT. This ensures that terminated or old employees do not still have access to the system. *No issues noted.*

### **STEP 5: Test Key General IT Controls:**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Key Control #3 (Manual)

*Prepared By:* NJH, 7/1/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion:
---------------------

### **Purpose:**

To confirm whether The Financial Consultant at WSDOT's headquarters' Accounting and Finance Division prepares the Inventory Systems vs. TARTS Analysis to verify the Capital Facilities Historical cost and Accumulated Depreciation from Facility Inventory Division (CAFM) agrees with the data shown in TARTS for **Key Control #3 for Buildings - TRAINS/CAFM** in order to assess control risk.

# State of Washington

## **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

## State of Washington

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #3 (Valuation):** The Financial Consultant at WSDOT's headquarters' Accounting and Finance Division prepares the Inventory Systems vs. TARTS Analysis to verify the Capital Facilities Historical cost and Accumulated Depreciation from Facility Inventory Division (CAFM) agrees with the data shown in TARTS.

The understanding for this system is documented above in the [[Controls - Buildings - TRAINS/CAFM](#)] step.

### **1. Confirmation of Key Manual Control:**

We received a copy of the April 2024 Inventory Systems vs. TARTS Analysis on from Jesse Daniels, Audit Liaison, on behalf of Suzi Freelund, Accounting & Reporting Manager. The spreadsheet shows a query for the amount (historical cost) and depreciation (accumulated depreciation) for the current month sorted by the respective inventory system used by capital assets. A pivot table is created based on the data and sorted by the 9 different distinct inventory systems which are as follows:

- Facilities
- Facilities/MC Facilities
- FEMS
- IRIS
- MC
- Remedy
- Terminals
- Vessels
- WAIMS

A "TARTS Variance" section is set up adjacent to the pivot table to analyze the comparison between the calculated pivot table sums and what is

## State of Washington

shown on an external TART report. By analyzing the excel formula used for the "Facilities" system, "`=389352955-GETPIVOTDATA("Sum of Amount",$J$1,"Inventory System","Facilities")`" we were able to understand that the TARTS figures are manually hard keyed into each formula from each external TARTS report which is referenced/documentated adjacent to each cell. Any discrepancies & variances are usually noted by the editor of the spreadsheet. ***No issues noted.***

Additionally, we noted that the total for the "Facilities" and "MC Facilities" systems (we omitting other line items not a part of Capital Facilities), the total cost was \$389,359,553.00 and the total A/D was \$162,258,073.50. The total manually entered TARTS amounts showed \$389,352,955 in costs and \$162,251,575 in A/D. Therefore, the noted variances in the spreadsheet for these systems were \$6,598 and \$6,498 respectively. The editor noted in the spreadsheet that there is a regular permanent difference of these amounts between Facilities & MC Facilities. ***No issues noted.***

We were able to confirm that the Inventory Systems vs. TARTS Analysis verified the Capital Facilities Historical cost and Accumulated Depreciation from Facility Inventory Division (CAFM) and that it agrees with the data shown in TARTS. ***No issues noted.***

### **Noted Weaknesses are as follows:**

**None**

### **2. Preliminary Control Risk Assessment**

MAX - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Key Control #4 - TRAINS/AFRS (Manual)

*Prepared By:* NJH, 7/11/2024

*Reviewed By:* RKM, 10/14/2024

## State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm whether the Accounting and Reporting unit performs monthly TRAINS/AFRS fund and GL reconciliations to ensure transactions are properly reported within AFRS for **Key Control #4 for TEF - TRAINS/FEMS and Buildings - TRAINS/CAFM** in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent

## State of Washington

material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. *Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. *Controls are not related to a "significant risk" identified in the audit plan.*



## State of Washington

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #1 (Valuation):** The Accounting and Reporting unit performs monthly TRAINS/AFRS fund and GL reconciliations to ensure transactions are properly reported within AFRS.

The understanding for this control/system is documented in the "Controls - TEF - TRAINS/FEMS" and "Controls - Buildings - TRAINS/CAFM" steps as this control pertains to these DOT systems regarding depreciable assets.

An updated understanding of all systems was gained through a control confirmation walkthrough meeting with Suzi Freelund, Accounting & Reporting Manager, on 7/9/24. During this meeting we learned that Suzi (in place currently for Beth De Vaul) and her team do the general system wide vs. TARTS report reconciliations while each respective asset system manager for TEF (Charleen Emmons), Buildings (Krystle Mize) , and WSF (Eric Bozarth) do their own separate monthly reconciliations with TARTS Reports vs. TRAINS before Suzi & the accounting/reporting team do their reconciliation.

### **1. Confirmation of Key Manual Control:**

To confirm this key control, we observed a walkthrough from Suzi Freelund, Accounting & Reporting Manager, on 7/9/24 for the Month of April 2024 as well as inspected a copy of the *Inventory Systems vs. TARTS Report* for the month of April. From our understanding of the document and the walkthrough, we were able to identify that Suzi pulls the GL/Fund data in TRAINS (which uploads to AFRS every night) at the end of each month and reconciles these amounts to the pulled TARTS reports from each system. From here she will inspect any variances in total cost and

## State of Washington

total accumulated depreciation based on the nine different internal asset systems in TRAINS. There were two variances she went through for the "Facilities" and "MC Facilities" systems identified in April which she noted are "always offset" due to accounting differences that exist between facility assets and minor capital assets. The total cost was \$389,359,553.00 and the total A/D was \$162,258,073.50 for both systems. The total TARTS amounts showed \$389,352,955 in costs and \$162,251,575 in A/D. Therefore, the noted trivial variances in the spreadsheet for these systems were \$6,598 and \$6,498 respectively that she addressed. ***No issues noted.***

Suzi had us note here that this is a completely separate process than the quarterly reconciliation process done by Beth De Vul who enters the depreciation amounts into TRAINS, then creates TRAINS and AFRS journal vouchers to record the increase or decrease in asset balances and depreciation in both financial systems.

During our walkthrough Suzi also pulled up a copy of a TRAINS reconciliation spreadsheet used to reconcile TARTS reports amounts and TRAINS amounts for Minor Capitalization projects (MC) and Remedy projects (IT Assets). Suzi explained that this sheet helps her identify any variances or discrepancies, and that if a variance or issue is found, she will send the information over to the specified region where the variance took place. Note here that Minor Capital and IT Assets are not included in the scope of our audit but does provide additional context as to the control environment regarding DOT assets. ***No issues noted.***

### **Noted Weaknesses are as follows:**

**None**

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Controls - WSF - TRAINS

*Prepared By:* NJH, 6/20/2024

*Reviewed By:* RKM, 10/14/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant

## State of Washington

deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- Initiation:* How are transactions initiated?
- Authorization:* How are transactions and accounting record maintenance authorized?
- Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

# State of Washington

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Material Balance and Assertions**

Internal controls in the TRAINS system address the following balance:

Depreciable Assets (Net of Depreciation)

For the following assertions:

Existence - The furnishings, equipment and capitalized costs have been disposed, replaced or otherwise impaired.

Valuation - The amount reported for this line item does not represent actual capitalized costs of furnishings and equipment constructed, purchased, or donated as of the report date.

Valuation - Newly added furnishings and equipment are not stated at historical or estimated historical cost.

Valuation - Depreciation may be incorrectly calculated because the wrong asset class code or useful life is entered into the system.

Significant Accounting System:

# State of Washington

**Transportation Reporting and Accounting and Information System (TRAINS)** - TRAINS is used to post expenditures using Payment Vouchers or Journal Vouchers. TRAINS does not allow the creator to review and approve their own work.

## Other Systems (Not Significant Systems):

**Transportation Assets Reporting and Tracking System (TARTS)** - Text file from FEMS, showing value and life-to-date depreciation from capital asset inventory systems.

**COGNOS Datamart and Financial Information Retrieval System (FIRS)** - Read only systems used to access WSDOT accounting system expenditures in the capitalization process.

## **Purchase and Capitalization of Transportation Equipment:**

We met with the following staff on 5/13/24 to discuss the purchase and capitalization controls related to ferries:

Eric Bozarth - WSF Capital Accountant

Lewis Bequette - Controller at WSF

Beth De Vault - AFS Transportation Financial Consultant

Suzi Freelund - Accounting and Reporting Manager

Loretta Sexton - Expenditures manager at WSF

Jesse Daniels - WSDOT Audit Liaison

Washington State Ferries (WSF) only tracks the vessels, equipment attached to the vessels, and the ferry terminals; the smaller equipment such as power equipment or vehicles are included in the Transportation Equipment Fund (TEF). They use an excel spreadsheet to track the equipment and calculate depreciation. The spreadsheet includes cost, acquisition date, useful life, remaining life, and monthly and accumulated depreciation calculations. Assets are added to the spreadsheet using data from the COGNOS report showing all capital expenses for the quarter.

## Additions

Quarterly, WSF will update the Excel spreadsheet for vessels, terminals, and make updates to the construction in progress (CIP) excel spreadsheet. The WSF Capital Accountant (Eric Bozarth) will run a COGNOS report for all capital expenses for the quarter and reach out to the vessels and terminals business groups to obtain a list of new CIP work orders. The vessel and terminal business groups will also leave notes for completed projects, useful life, and when it was completed. The information in the Excel spreadsheet for CIP is updated for the new quarter, so the beginning balance equals the previous quarter's ending balance. Once the file is updated the WSF Capital Accountant adds in the COGNOS data, which will contain any additions and their amounts from the quarter. The WSF Capital Accountant will work with the vessels or terminals business groups to determine which projects are complete and should be added to the vessel asset spreadsheet, and which costs should be added to construction in progress (**Key Control #1 - Existence**).

## Deletions

Deletions of vessels and terminals are rare, due their long expected useful life. There are three vessels awaiting sale and are off of the WSF books

## State of Washington

and noted in the disclosures for FY23.

### Depreciation Calculation

The monthly depreciation calculation is tracked in the WSF Vessels Fixed Asset spreadsheet and is based on the useful life and data provided by the ferries and vessels business groups (useful life, cost, and project complete date). The monthly depreciation is added to the accumulated depreciation, which is recorded via journal entry **(Key Control #2 - Valuation)**.

### **How Transactions are Recorded in AFRS:**

At the end of the quarter Beth De Vul, Transportation Financial Consultant, uses the WSF Vessels Spreadsheet and WSF Terminals Spreadsheet and creates the "Department of Transportation Fixed Asset Detail Report (HWY-RAI06060A)". This report is compared to the WSF report maintained by Eric Bozarth. Changes from the WSF Fixed Assets Excel spreadsheet and construction in progress that occurred in the quarter are recorded by Beth through a JV into TRAINS and AFRS **(Key Control #3 - Valuation)**.

### **Key Controls are as Follows:**

**Key Control 1 - Valuation:** WSF tracks depreciation in the WSF Vessels Fixed Assets Excel spreadsheet based on cost and useful life for each vessel.

**Key Control 2 - Existence/Valuation:** Each quarter, the Transportation Financial Consultant creates the "Department of Transportation Fixed Asset Detail Report". This report is compared to the WSF report maintained by the WSF Capital Accountant, changes (additions/reductions) and construction in progress that occurred in the quarter are recorded by the Financial Consultant through a JV into TRAINS and AFRS.

### **Noted Weaknesses are as Follows:**

None

### I.3.PRG - Depreciable Assets (Net of Depreciation)

*Procedure Step:* Key Control #1 (Manual)

*Prepared By:* NJH, 7/2/2024

*Reviewed By:* RKM, 7/5/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm whether WSF tracks depreciation in the WSF Vessels Fixed Assets Excel spreadsheet based on cost and useful life for each vessel for **Key Control #1 for Ferries - TRAINS/FEMS** in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent



## State of Washington

material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. *Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. *Controls are not related to a "significant risk" identified in the audit plan.*

## State of Washington

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control #1 (Valuation):** WSF tracks depreciation in the WSF Vessels Fixed Assets Excel spreadsheet based on cost and useful life for each vessel.

The understanding for this system is documented above in the "Controls - WSF - Trains" step.

### **1. Confirmation of Key Manual Control:**

To confirm the key control, we obtained a copy of the WSF Vessels Fixed Assets spreadsheet [[WSF Vessels Fixed Assets Excel spreadsheet \(PBC\)](#)] from Jesse Daniels, Audit Liaison, on behalf of Lewis Bequette, WSF Controller. Upon reviewing the spreadsheet, we noted the spreadsheet includes vessel details including name of vessel, addition and related work orders, acquisition date, and cost. We recalculated the monthly depreciation for WO 00-4173 for the Tillikum asset "Renovation" and found that it matched the depreciation expense recorded for that month as well as tied to the total accumulated depreciation up to April '24. The spreadsheet also has columns for Accumulated Depreciation (March), Depreciation & Accumulated Depreciation (April), and Annual Deprecation. We noted the March accumulated + April monthly matched the April accumulated depreciation as expected. We were able to confirm WSF is using their Fixed Asset Reporting Excel spreadsheet to track depreciation and cost for each vessel. *No issues noted.*

**Noted Weaknesses are as follows:**

# State of Washington

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

*Procedure Step:* Key Control #2 (Manual)

*Prepared By:* NJH, 7/12/2024

*Reviewed By:* SHW, 7/25/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm whether Each quarter, the Transportation Financial Consultant creates the "Department of Transportation Fixed Asset Detail Report". This report is compared to the WSF report maintained by the WSF Capital Accountant, changes (additions/reductions) and construction in progress that occurred in the quarter are recorded by the Financial Consultant through a JV into TRAINS and AFRS (**Key Control #2 for Ferries - TRAINS**) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

## State of Washington

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

## State of Washington

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

**Key Control #2 (Existence/Valuation):** Each quarter, the Transportation Financial Consultant creates the "Department of Transportation Fixed Asset Detail Report". This report is compared to the WSF report maintained by the WSF Capital Accountant, changes (additions/reductions) and construction in progress that occurred in the quarter are recorded by the Financial Consultant through a JV into TRAINS and AFRS.

The understanding for this system is documented above in the "Controls - WSF - Trains" step.

## **1. Confirmation of Key Manual Control:**

To confirm this control we reviewed *JV31C00000046081 - Vessels* for March Q3 changes in vessel CIP and depreciation. The total JV amount for Vessels was \$9,600,325.65 with CIP additions of \$1,399,662.17 and depreciation expense of \$8,200,663.48. These are details provided within the JV. The CIP and depreciation totals tied to the total bottom line for *March WSF Fixed Asset Report* (maintained by Eric Bozarth) and the *WSF Buildings & Vessels Quarterly Adj.* The accounts that were debited/credited were reasonable based on the line items of the transactions. ***No issues noted.***

This JV was prepared by Beth De Vault (AFS Transportation Financial Consultant) on 4/29/2024 and approved that same day by Suzi Freeland (Accounting & Reporting Manager). ***No issues noted.***

## **Noted Weaknesses are as follows:**

**None**

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.3.PR.G - Depreciable Assets (Net of Depreciation)**

# State of Washington

*Procedure Step:* Risk Assessment

*Prepared By:* NJH, 8/28/2024

*Reviewed By:* RKM, 8/28/2024

Purpose/Conclusion:

**Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

*General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

*Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

## State of Washington

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.



## State of Washington

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Existence - High

Valuation - High

# State of Washington

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**TEF - TRAINS/FEMS: (Valuation/Existence)**

**Buildings - TRAINS/CAFM: (Valuation/Existence)**

**WSF - TRAINS: (Valuation/Existence)**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Existence - High

Valuation - High

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

### **TEF:**

(Existence) - We will select a sample of TEF equipment and verify existence by reviewing photos/recent work orders.

(Valuation) - Verify a sample of monthly TRAINS/AFRS Depreciation Reconciliations are completed to ensure balances are valued correctly.

(Valuation) - Recalculate a sample of asset depreciation amounts to confirm FEMS is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets.

### **Buildings:**

(Existence) - We will select a sample of capital assets and verify existence by reviewing photos/recent work orders.

(Valuation) - Recalculate a sample of asset depreciation amounts to confirm CAFM is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets.

# State of Washington

## WSF:

- (Existence) - Select all vessels from the asset listing to determine whether they exist by viewing VesselWatch which records ferry location and activity.
- (Valuation) - Recalculate accumulated depreciation & net book value for all WSF Vessels from the asset listing. Additionally, we will compare the useful life code against the relevant SAAM commodity code to ensure useful life is appropriate for vessels used in the calculation.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## I.3.PRG - Depreciable Assets (Net of Depreciation)

*Procedure Step:* Substantive Test - TEF (TRAINS/FEMS)  
*Prepared By:* NJH, 10/17/2024  
*Reviewed By:* CJG, 12/5/2024

Purpose/Conclusion.*
----------------------

### **Purpose - Existence:**

To determine whether reported capital assets represent real assets, as of the end of the period.

### **Conclusion:**

We determined that the TEF assets currently exist and represents real asset obligations as of the reporting date. *No issues noted.*

### **Purpose - Valuation:**

To determine whether capital assets are reported at properly valued and calculated amounts.

### **Conclusion:**

We determined the monthly reconciliations to be accurate and performed timely and that FEMS is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets. *No issues noted.*

# State of Washington

## Testing Strategy:

### Valuation:

The following is a list of **considerations** for testing the valuation assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### Incorrect Depreciation Calculations

Perform an analytical review of depreciation expense by type of asset for reasonableness.

Re-calculate depreciation expense for a sample of assets or in conjunction with a test of automated controls (if depreciation is automatically calculated by the system). Consider testing the inputs used for the calculation to determine whether they are reasonable and in line with any applicable policies; i.e. useful life, salvage value, etc. Alternatively, test calculations, extensions and footing of subsidiary records if records are maintained on spreadsheets.

Evaluate capital asset policies for componentization or grouping of assets to determine if it has been consistently followed and will result in a rational method of depreciation. See BARS [3.3.10.150](#) for guidance.

Evaluate estimated useful life and scrap value factors for reasonableness. This test could be done in general (on the government's accounting policies), for selected asset classes or for selected or sampled asset records.

*If testing selected high risk assets, auditors should consider assets that are nearly or fully depreciated (see BARS [3.3.10.130](#)), assets with unusually high or low useful lives for their type, and assets with unusually high scrap values.*

Compare estimated useful lives for assets with replacement schedules / policies and capital budgets.

*We would expect that assets on a regular replacement schedule (such as equipment, vehicles, road surfacing, etc) or that are included for replacement in the capital budget would have estimated useful lives that match the government's replacement plans for the asset.*

Consider whether the date placed in service for assets is reasonable given when the asset begins being used or is substantially complete as this will have an effect on when depreciation begins. See information in BARS [3.3.10.90](#) about when to move a project out of CIP.

### Impairment

Check that the measurement method used for write-offs is in accordance with GAAP (GASB 42.12-15). Review or recalculate the portion of historical cost that should be written off for impaired capital assets. *Note: auditor would normally use the same measurement method used by the government unless it the auditor finds it inappropriate for the circumstances or unallowable under GAAP.*

### Incorrect Historical Cost of Assets

# State of Washington

Trace recorded cost to supporting documentation. *Note: This test would normally be limited to recent additions, since documentation for historical assets has likely passed the records retention period.*

Evaluate the reasonableness of any estimates of the historical cost of capital assets.

Evaluate the reasonableness and support for any estimates of the acquisition value (per GASB 72) of donated capital assets.

## **Conversion to GAAP**

For governments converting to GAAP reporting, examine valuation method for retroactively reported infrastructure assets and verify that the valuation method used is one of the methods prescribed by the County Road Advisory Board.

## **Modified Approach**

Check that infrastructure is being depreciated unless the modified approach is used. If the modified approach is used, verify that the government has met criteria of GASB 34 par 23-26.

## **Allocation**

On the government-wide statement of activities, review allocation of depreciation for capital assets for governmental funds. Depreciation expense will be reported as a component of the direct expense shown in the statement of activities. Request spreadsheet for allocation.

Existence:

The following is a list of **considerations** for testing the existence assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Nonexistent Assets**

Review capital asset records to determine whether records meet minimum requirements of BARS [3.3.9.40](#) to positively identify and adequately describe the asset. If asset records are not sufficient, follow up on how the entity is able to identify and track reported assets and consider further audit procedures.

Scan the capital asset list for unusual or unexpected assets or patterns.

*For example: asset descriptions that appear insufficient to identify the asset, asset descriptions that seem strange, assets with a historical cost that doesn't appear to meet the capital asset threshold, assets that are past the end of their service life, assets or asset types that don't appear to belong (based on auditor's understanding of entity activities and area of operation), assets or asset types that the auditor doesn't recognize, attributes that appear unreasonable (historical cost, useful life or scrap value), assets that appear connected to actions noted in planning procedures (impairment, replacement, sale or surplus, transfer), etc.*

## State of Washington

Test sampled assets or selected high-risk assets from accounting records for existence by observing them or reviewing documentation.

*Observation for aboveground infrastructure such as roads, bridges or buildings may be by [google maps](#). Documentation for underground assets may consist of maps, system plans approved by regulatory agencies or permits, etc.*

Review the government's records of the latest physical inventory for any identification and follow-up on missing assets or any types of assets or locations that were not covered. Note: review of a government's physical inventory is considered a control test. However, it may be done as a risk assessment procedure to help direct substantive testing, and follow-up on results may result in some substantive evidence.

Trace assets from accounting records to assets listed on the government's insurance policy records. Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

Trace assets from accounting records to operational records (ex: Public Works Department typically tracks assets for maintenance or regulatory reporting purposes). Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

For land and buildings, trace parcels and historical cost per the land subsidiary schedules to the County's land (GIS) records to verify ownership. Note: this test also provides evidence for the rights & obligations assertion and - if a complete list is obtained from the County - for the completeness assertion as well.

Compare reported public project completed or in process during the period to the L&I [prevailing wage reporting database](#). Note: since reporting is done by contractors, it would be considered a third-party verification of project existence. We would expect capitalized costs (which include costs incurred by the government as well as contractors) to exceed the contractor's reported costs for most projects. This test also provides evidence for the completeness assertion if traced from the L&I database.

### **Cut-off**

Review supporting documentation to verify dates of any transfers, annexations or donations.

See the Expenditures | Existence step for testing strategies on cut-off for capitalized expenditures.

### **Detail Roll-Up**

If manual journal entries are required to update the GL, agree figures per the GL to subsidiary schedules or systems.

Search for manual journal entries that debit (increase) capital or infrastructure assets. Consider testing if any risk indicators are noted.

Reconcile (or review the government's reconciliation) capital expenditures for governmental funds to increases in capital assets. The only anticipated reconciling item would be equipment that is below the capitalization threshold.

Reconcile (or review the government's reconciliation) increases in capital assets to capital purchases and sales per the statement of cash flows for proprietary funds. The only anticipated reconciling item would be donated or contributed assets.

# State of Washington

**Over/Invalid Capitalization** - See classification step for testing strategies on improper capitalization upon construction or acquisition, or when determining whether an expense is a maintenance or repair expense or a capitalized improvement.

## **Unrecorded Disposals or Impairments**

Scan capital asset records for fully depreciated assets and inquire as to the status (disposed, no longer in use, etc.) to ensure all retirements and disposals have been recorded. Evaluate appropriate accounting for any fully depreciated assets remaining in service in accordance with [BARS 3.3.10.130](#).

Identify significant disposals, impairments (due to obsolescence or damage) or contributions per review of minutes and trace to asset records to verify these events were accounted for.

Request a list of insurance claims made during the audit period to identify possible impairments or removed assets, then trace to subsidiary records to verify that the event was properly accounted for.

Identify annexations (through minutes, inquiry or OFM's central annexation tracking system) and trace to supporting documents showing the transfer of assets. Note: this test would also provide evidence for the completeness and rights & obligations assertions.

## **Joint Ventures**

Evaluate involvement in undivided interests, joint ventures, jointly governed organizations, and component units (identified as part of the perm file and Reporting Entity step) for assets that may have been jointly acquired, constructed or used (see [BARS 3.3.10.20](#)).

See the Rights & Obligations step for additional testing strategies related to capital assets being transferred between governments or created as part of joint projects.

Guidance/Criteria:
--------------------

### **Existence:**

#### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

## **BARS [3.3.9](#) Capital Asset Management System Requirements**

GAAP criteria for reporting capital assets

[GASB Codification Section 1400](#) Reporting Capital Assets

[GASB Comprehensive Implementation Guide Chapter 7](#) Basic Financial Statements and Management's Discussion and Analysis, sections 7.9-7.21

### **Valuation:**

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

2012 GAAFR page 451 describes generally accepted estimation methods for when the historical cost of an asset is unknown. NOTE: The County Road Advisory Board (CRAB) worked with local governments to develop several methods for valuing historical infrastructure assets when GASB 34 was implemented.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.3.9](#) Capital Asset Management System Requirements**

**BARS [3.3.10](#) Capital Asset Accounting** - guidance on determining ownership of capital assets.

**BARS [3.9.2](#) Property Transfers**

GAAP criteria for reporting capital assets

**[GASB Codification Section 1400](#) Reporting Capital Assets**

**[GASB Comprehensive Implementation Guide Chapter 7](#) Basic Financial Statements and Mangement's Discussion and Analysis, sections 7.9-7.21**

Record of Work Done.:

### **Substantive tests performed to meet the Existence assertion:**

(Existence) - We will select a sample of TEF equipment and verify existence by reviewing photos/recent work orders.

We used the FS Sampling Spreadsheet to select a sample of TEF equipment for testing using the random number generator. Using a tolerable misstatement of 7.5%, assurance at high, we determined a sample size of 39 randomly selected TEF items. Charleen Emmons, Fleet Operations Budget and Finance Manager, provided us with images on 08/08/24 of each selected TEF asset selected for testing. We were able to review each photo to confirm that the asset currently exists and represents real asset obligations as of the reporting date. See testing at [[TEF Testing \(Existence & Valuation\)](#)]. *No issues noted.*

### **Substantive tests performed to meet the two Valuation assertions:**

(Valuation) - Verify a sample of monthly TRAINS/AFRS Depreciation Reconciliations are completed to ensure balances are valued correctly.



## State of Washington

We used the FS Sampling Spreadsheet for Populations of 365 or less to test FEMS to TRAINS reconciliations for TEFS equipment. Using a tolerable misstatement of 7.5% and setting assurance at High, we determined a sample size of 5 monthly reconciliations. Charleen Emmons, Fleet Operations Budget and Finance Manager, provided us with the reconciliations and the JVs to correct the variances between the two systems. We found the reconciliations to be accurate and performed timely. We confirmed ACFR tie out and population completeness by comparing the PBC report to the *TRAINS Trial Balance Report A613B dated 8/29/24* for funds 997 & 410 with variances below the floor. See testing at [\[TEF Testing \(Existence & Valuation\)\]](#). ***No issues noted.***

(Valuation) - Recalculate a sample of asset depreciation amounts to confirm FEMS is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets.

We used the FS Sampling Spreadsheet to select a sample of TEF equipment for testing using the random number generator. Using a tolerable misstatement of 7.5%, assurance at high, we determined a sample size of 39 randomly selected TEF items. Charleen Emmons, Fleet Operations Budget and Finance Manager, provided us with an export from the TARTS system, detailing all TEF Capital Assets, as of 6/30/2024. We recalculated asset depreciation amounts to confirm FEMS is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets. We noted differences below the floor. Additionally, we confirmed ACFR tie out and population completeness by comparing the PBC report to the *TRAINS Trial Balance Report A613B dated 8/29/24* for funds 997 & 410 with variances below the floor. See testing at [\[TEF Testing \(Existence & Valuation\)\]](#). ***No issues noted.***

### I.3.PRG - Depreciable Assets (Net of Depreciation)

***Procedure Step:*** Substantive Test - Buildings (TRAINS/CAFM)

***Prepared By:*** NJH, 10/17/2024

***Reviewed By:*** CJG, 12/5/2024

Purpose/Conclusion:
---------------------

**Purpose - Existence:**

To determine whether reported capital assets represent real assets, as of the end of the period.

**Conclusion:**

We determined that the capital facility assets currently exist and represents real asset obligations as of the reporting date. ***No issues noted.***

# State of Washington

## **Purpose - Valuation:**

To determine whether capital assets are reported at properly valued and calculated amounts.

## **Conclusion:**

We determined the CAFM is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets withx noted differences below the floor. ***No issues noted.***

## Testing Strategy:

The following is a list of **considerations** for testing the valuation assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Incorrect Depreciation Calculations**

Perform an analytical review of depreciation expense by type of asset for reasonableness.

Re-calculate depreciation expense for a sample of assets or in conjunction with a test of automated controls (if depreciation is automatically calculated by the system). Consider testing the inputs used for the calculation to determine whether they are reasonable and in line with any applicable policies; i.e. useful life, salvage value, etc. Alternatively, test calculations, extensions and footing of subsidiary records if records are maintained on spreadsheets.

Evaluate capital asset policies for componentization or grouping of assets to determine if it has been consistently followed and will result in a rational method of depreciation. See BARS [3.3.10.150](#) for guidance.

Evaluate estimated useful life and scrap value factors for reasonableness. This test could be done in general (on the government's accounting policies), for selected asset classes or for selected or sampled asset records.

*If testing selected high risk assets, auditors should consider assets that are nearly or fully depreciated (see BARS [3.3.10.130](#)), assets with unusually high or low useful lives for their type, and assets with unusually high scrap values.*

Compare estimated useful lives for assets with replacement schedules / policies and capital budgets.

*We would expect that assets on a regular replacement schedule (such as equipment, vehicles, road surfacing, etc) or that are included for replacement in the capital budget would have estimated useful lives that match the government's replacement plans for the asset.*

Consider whether the date placed in service for assets is reasonable given when the asset begins being used or is substantially complete as this will have an effect on when depreciation begins. See information in BARS [3.3.10.90](#) about when to move a project out of CIP.

# State of Washington

## **Impairment**

Check that the measurement method used for write-offs is in accordance with GAAP (GASB 42.12-15). Review or recalculate the portion of historical cost that should be written off for impaired capital assets. *Note: auditor would normally use the same measurement method used by the government unless it the auditor finds it inappropriate for the circumstances or unallowable under GAAP.*

## **Incorrect Historical Cost of Assets**

Trace recorded cost to supporting documentation. *Note: This test would normally be limited to recent additions, since documentation for historical assets has likely passed the records retention period.*

Evaluate the reasonableness of any estimates of the historical cost of capital assets.

Evaluate the reasonableness and support for any estimates of the acquisition value (per GASB 72) of donated capital assets.

## **Conversion to GAAP**

For governments converting to GAAP reporting, examine valuation method for retroactively reported infrastructure assets and verify that the valuation method used is one of the methods prescribed by the County Road Advisory Board.

## **Modified Approach**

Check that infrastructure is being depreciated unless the modified approach is used. If the modified approach is used, verify that the government has met criteria of GASB 34 par 23-26.

## **Allocation**

On the government-wide statement of activities, review allocation of depreciation for capital assets for governmental funds. Depreciation expense will be reported as a component of the direct expense shown in the statement of activities. Request spreadsheet for allocation.

Guidance/Criteria:
--------------------

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

2012 GAAFR page 451 describes generally accepted estimation methods for when the historical cost of an asset is unknown. NOTE: The County Road Advisory Board (CRAB) worked with local governments to develop several methods for valuing historical infrastructure assets when GASB 34 was implemented.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

# State of Washington

## **BARS [3.3.9](#) Capital Asset Management System Requirements**

**BARS [3.3.10](#) Capital Asset Accounting** - guidance on determining ownership of capital assets.

## **BARS [3.9.2](#) Property Transfers**

GAAP criteria for reporting capital assets

**[GASB Codification Section 1400](#) Reporting Capital Assets**

**[GASB Comprehensive Implementation Guide Chapter 7](#) Basic Financial Statements and Mangement's Discussion and Analysis, sections 7.9-7.21**

Record of Work Done.

### **Substantive tests performed to meet the Existence assertion:**

(Existence) - We well make a selection of capital assets and verify existence by reviewing photos/recent work orders.

We used the FS Sampling Spreadsheet to select a sample of Capital Facilities assets for testing using the random number generator. Using a tolerable misstatement of 7.5%, assurance at high, we determined a sample size of 38 randomly selected Facility assets. Krystle Mize, Capital Facilities Financial Manager, provided us with images on 08/12/24 of each selected facilities asset selected for testing. We were able to review each photo to confirm that the asset currently exists and represents a real asset obligation as of the reporting date. See testing at [[Buildings Testing \(Existence & Valuation\)](#)]. ***No issues noted.***

### **Substantive tests performed to meet the Valuation assertion:**

(Valuation) - Recalculate selection of asset depreciation amounts to confirm CAFM is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets.

We used the FS Sampling Spreadsheet to select a sample of TEF equipment for testing using the random number generator. Using a tolerable misstatement of 7.5%, assurance at high, we determined a sample size of 38 randomly selected Facility assets. Elena Fehr, IT Data Management - Facilities, provided us with an export from the TARTS system on 8/8/24, detailing all capital facility assets, as of 6/30/2024. We recalculated asset accumulated depreciation and monthly depreciation amounts to confirm CAFM is automatically populating an accurate amount based on inventory value, LTD amount, salvage value, and useful life remaining of assets. We noted differences below the floor. Additionally, we confirmed ACFR tie out and population completeness by comparing the PBC report to the *TRAINS Trial Balance Report A613B dated 8/29/24* for funds 997 & 410 with varainces below the floor. See testing at [[Buildings Testing \(Existence & Valuation\)](#)]. ***No issues noted.***

Based on our recalculation misstatement found during control work, we chose to discuss all variances presented during testing with agency. The agency noted that the CAFM system was not recording any cents/decimal values over the years, creating cumulative rounding variances for both

## State of Washington

the monthly depreciation and accumulated depreciated amounts. Additionally, there were 5 assets by which the agency noted that they will need to investigate further as to why the monthly depreciation amounts appear to be off from our recalculations as there was no immediate explanation. All of the rounding variances noted were corrected and adjusted in an additional TARTS report dated for 7/30/24 after year-end which is outside the scope of our testing. We analyzed both the updated depreciation amounts and the original testing amounts and have noted that the variances from both recalculations are below the floor and neither variances represent a significant misstatement. ***No issues noted.***

### I.3.PRG - Depreciable Assets (Net of Depreciation)

*Procedure Step:* Substantive Test - WSF (TRAINS/FEMS)

*Prepared By:* NJH, 10/17/2024

*Reviewed By:* CJG, 12/5/2024

#### Purpose/Conclusion:

##### **Purpose - Existence:**

To determine whether reported capital assets represent real assets, as of the end of the period.

##### **Conclusion:**

We determined that the reported capital assets represent real assets, as of the end of the period. ***No issues noted.***

##### **Purpose - Valuation:**

To determine whether capital assets are reported at properly valued and calculated amounts.

##### **Conclusion:**

We determined that the capital assets are reported at properly valued and calculated amounts. ***No issues noted.***

#### Testing Strategy:

The following is a list of **considerations** for testing the valuation assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Incorrect Depreciation Calculations**

## State of Washington

Perform an analytical review of depreciation expense by type of asset for reasonableness.

Re-calculate depreciation expense for a sample of assets or in conjunction with a test of automated controls (if depreciation is automatically calculated by the system). Consider testing the inputs used for the calculation to determine whether they are reasonable and in line with any applicable policies; i.e. useful life, salvage value, etc. Alternatively, test calculations, extensions and footing of subsidiary records if records are maintained on spreadsheets.

Evaluate capital asset policies for componentization or grouping of assets to determine if it has been consistently followed and will result in a rational method of depreciation. See BARS [3.3.10.150](#) for guidance.

Evaluate estimated useful life and scrap value factors for reasonableness. This test could be done in general (on the government's accounting policies), for selected asset classes or for selected or sampled asset records.

*If testing selected high risk assets, auditors should consider assets that are nearly or fully depreciated (see BARS [3.3.10.130](#)), assets with unusually high or low useful lives for their type, and assets with unusually high scrap values.*

Compare estimated useful lives for assets with replacement schedules / policies and capital budgets.

*We would expect that assets on a regular replacement schedule (such as equipment, vehicles, road surfacing, etc) or that are included for replacement in the capital budget would have estimated useful lives that match the government's replacement plans for the asset.*

Consider whether the date placed in service for assets is reasonable given when the asset begins being used or is substantially complete as this will have an effect on when depreciation begins. See information in BARS [3.3.10.90](#) about when to move a project out of CIP.

### **Impairment**

Check that the measurement method used for write-offs is in accordance with GAAP (GASB 42.12-15). Review or recalculate the portion of historical cost that should be written off for impaired capital assets. *Note: auditor would normally use the same measurement method used by the government unless it the auditor finds it inappropriate for the circumstances or unallowable under GAAP.*

### **Incorrect Historical Cost of Assets**

Trace recorded cost to supporting documentation. *Note: This test would normally be limited to recent additions, since documentation for historical assets has likely passed the records retention period.*

Evaluate the reasonableness of any estimates of the historical cost of capital assets.

Evaluate the reasonableness and support for any estimates of the acquisition value (per GASB 72) of donated capital assets.

### **Conversion to GAAP**

For governments converting to GAAP reporting, examine valuation method for retroactively reported infrastructure assets and verify that the

# State of Washington

valuation method used is one of the methods prescribed by the County Road Advisory Board.

## Modified Approach

Check that infrastructure is being depreciated unless the modified approach is used. If the modified approach is used, verify that the government has met criteria of GASB 34 par 23-26.

## Allocation

On the government-wide statement of activities, review allocation of depreciation for capital assets for governmental funds. Depreciation expense will be reported as a component of the direct expense shown in the statement of activities. Request spreadsheet for allocation.

Existence:

The following is a list of **considerations** for testing the existence assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## Nonexistent Assets

Review capital asset records to determine whether records meet minimum requirements of BARS [3.3.9.40](#) to positively identify and adequately describe the asset. If asset records are not sufficient, follow up on how the entity is able to identify and track reported assets and consider further audit procedures.

Scan the capital asset list for unusual or unexpected assets or patterns.

*For example: asset descriptions that appear insufficient to identify the asset, asset descriptions that seem strange, assets with a historical cost that doesn't appear to meet the capital asset threshold, assets that are past the end of their service life, assets or asset types that don't appear to belong (based on auditor's understanding of entity activities and area of operation), assets or asset types that the auditor doesn't recognize, attributes that appear unreasonable (historical cost, useful life or scrap value), assets that appear connected to actions noted in planning procedures (impairment, replacement, sale or surplus, transfer), etc.*

Test sampled assets or selected high-risk assets from accounting records for existence by observing them or reviewing documentation.

*Observation for aboveground infrastructure such as roads, bridges or buildings may be by [google maps](#). Documentation for underground assets may consist of maps, system plans approved by regulatory agencies or permits, etc.*

Review the government's records of the latest physical inventory for any identification and follow-up on missing assets or any types of assets or locations that were not covered. Note: review of a government's physical inventory is considered a control test. However, it

## State of Washington

may be done as a risk assessment procedure to help direct substantive testing, and follow-up on results may result in some substantive evidence.

Trace assets from accounting records to assets listed on the government's insurance policy records. Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

Trace assets from accounting records to operational records (ex: Public Works Department typically tracks assets for maintenance or regulatory reporting purposes). Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

For land and buildings, trace parcels and historical cost per the land subsidiary schedules to the County's land (GIS) records to verify ownership. Note: this test also provides evidence for the rights & obligations assertion and - if a complete list is obtained from the County - for the completeness assertion as well.

Compare reported public project completed or in process during the period to the L&I [prevailing wage reporting database](#). Note: since reporting is done by contractors, it would be considered a third-party verification of project existence. We would expect capitalized costs (which include costs incurred by the government as well as contractors) to exceed the contractor's reported costs for most projects. This test also provides evidence for the completeness assertion if traced from the L&I database.

### **Cut-off**

Review supporting documentation to verify dates of any transfers, annexations or donations.

See the Expenditures | Existence step for testing strategies on cut-off for capitalized expenditures.

### **Detail Roll-Up**

If manual journal entries are required to update the GL, agree figures per the GL to subsidiary schedules or systems.

Search for manual journal entries that debit (increase) capital or infrastructure assets. Consider testing if any risk indicators are noted.

Reconcile (or review the government's reconciliation) capital expenditures for governmental funds to increases in capital assets. The only anticipated reconciling item would be equipment that is below the capitalization threshold.

Reconcile (or review the government's reconciliation) increases in capital assets to capital purchases and sales per the statement of cash flows for proprietary funds. The only anticipated reconciling item would be donated or contributed assets.

**Over/Invalid Capitalization** - See classification step for testing strategies on improper capitalization upon construction or acquisition, or when determining whether an expense is a maintenance or repair expense or a capitalized improvement.

### **Unrecorded Disposals or Impairments**

Scan capital asset records for fully depreciated assets and inquire as to the status (disposed, no longer in use, etc.) to ensure all retirements and disposals have been recorded. Evaluate appropriate accounting for any fully depreciated assets remaining in service in accordance with [BARS 3.3.10.130](#).



## State of Washington

Identify significant disposals, impairments (due to obsolescence or damage) or contributions per review of minutes and trace to asset records to verify these events were accounted for.

Request a list of insurance claims made during the audit period to identify possible impairments or removed assets, then trace to subsidiary records to verify that the event was properly accounted for.

Identify annexations (through minutes, inquiry or OFM's central annexation tracking system) and trace to supporting documents showing the transfer of assets. Note: this test would also provide evidence for the completeness and rights & obligations assertions.

### Joint Ventures

Evaluate involvement in undivided interests, joint ventures, jointly governed organizations, and component units (identified as part of the perm file and Reporting Entity step) for assets that may have been jointly acquired, constructed or used (see [BARS 3.3.10.20](#)).

See the Rights & Obligations step for additional testing strategies related to capital assets being transferred between governments or created as part of joint projects.

Guidance/Criteria:
--------------------

### Existence:

#### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.3.9](#) Capital Asset Management System Requirements**

GAAP criteria for reporting capital assets

[GASB Codification Section 1400](#) Reporting Capital Assets

[GASB Comprehensive Implementation Guide Chapter 7](#) Basic Financial Statements and Management's Discussion and Analysis, sections 7.9-7.21

### Valuation:

#### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

2012 GAAFR page 451 describes generally accepted estimation methods for when the historical cost of an asset is unknown. NOTE: The County Road Advisory Board (CRAB) worked with local governments to develop several methods for valuing historical infrastructure assets when GASB 34 was implemented.

# State of Washington

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.3.9](#) Capital Asset Management System Requirements**

**BARS [3.3.10](#) Capital Asset Accounting** - guidance on determining ownership of capital assets.

### **BARS [3.9.2](#) Property Transfers**

GAAP criteria for reporting capital assets

**[GASB Codification Section 1400](#) Reporting Capital Assets**

**[GASB Comprehensive Implementation Guide Chapter 7](#) Basic Financial Statements and Mangement's Discussion and Analysis, sections 7.9-7.21**

Record of Work Done.

#### **Substantive tests performed to meet the Existence assertion:**

(Existence) - Select all vessels from the asset listing to determine whether they exist by viewing VesselWatch which records ferry location and activity.

We selected ferry vessels from the WSF capital asset listing as of June 30, 2024 prepared by Eric Bozarth. We reviewed the asset dollar amount and asset type within the listing to determine whether the vessel was properly capitalized. We verified existence at <https://www.wsdot.com/ferries/vesselwatch/> as of 6/30/2024. See testing at [[WSF Testing \(Existence & Valuation\)](#)]. We noted all ferries existed as of fiscal year end. *No issues noted.*

#### **Substantive tests performed to meet the Valuation assertion:**

(Valuation) - Recalculate accumulated depreciation & net book value for all WSF Vessels from the asset listing. Additionally, we will compare the useful life code against the relevant SAAM commodity code to ensure useful life is appropriate for vessels used in the calculation.

We selected all vessel assets with \$661,051,569 in NBV, representing 100% of all WSF vessel assets. We tested for the net book value (arrived at by recalculating the accumulated depreciation) and the proper classification of the SAAM useful life to ensure the depreciation calculation was correct. We noted all assets were properly capitalized. We recalculated the net of depreciation amounts noting differences due to support not being provided for additions/disposals that occurred before 2019. Misstatement is below the floor individually and in aggregate. There were 31 instances where our recalculated "Asset Net of Depreciation" value did not match theirs. It was determined that these variances were caused by changes to the asset value that were not reported in the documentation we received. All of these additions/disposals took place before 2019 and there is no record to show evidence. Additionally, we confirmed ACFR tie out and population completeness by comparing the PBC report to the

# State of Washington

*TRAINS Trial Balance Report A613B dated 8/29/24 for funds 997 & 410 with variances below the floor. See testing at [[WSF Testing \(Existence & Valuation\)](#)]. The total variance was below the floor. **No issues noted.***

## I.4.PRG - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset

*Procedure Step:* Summary & Conclusion

*Prepared By:* MRF, 11/14/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the [Permanent File](#) by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

## State of Washington

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

## State of Washington

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **I.4.PRQ - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset**

*Procedure Step:* Understanding of Line Item

*Prepared By:* BM2, 5/20/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

# State of Washington

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account

## State of Washington

description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions:**

None.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

### **Balance Composition**

The Governmental Accounting Standards Board (GASB) issued GASB Statement No. 68, *Accounting and Financial Reporting for Pensions*, which revises and establishes new financial reporting for most governments that provide their employees with pension benefits. GASB Statement No. 68 is effective for financial statements for fiscal years beginning after June 30, 2014. Prior to implementing GASB 68, employers participating in an agent plan recognized annual pension cost under a funding approach. Pension expenses were derived from a measure of an annual required contribution to the plan. Pension liabilities resulted from the difference between contributions required and contributions made.

With the implementation of GASB 68, employers are now required to recognize a liability as employees earn their pension benefits. Employers participating in agent plans will recognize their specific pension amounts which include net pension liability, deferred outflows of resources, deferred inflows of resources, and pension expense.

Washington State defined benefit plans are defined as either:

Single-employer - those in which pension benefits are provided to the employees of only one employer.

# State of Washington

Cost-sharing, multiple-employer (cost-sharing) - those in which the pension obligations to the employees of more than one employer are pooled and pension plan assets can be used to pay the benefits of the employees of any employer that provides pensions through the pension plan.

We obtained the various retirement systems and plans in which the State of Washington employees participate by reviewing the prior year 2023 ACFR Note 15: Retirement Plans and from the 2023 Participating Employers Financial Information (PEFI) report. We summarized pension plans included in the line item and key attributes for each plan at [[Pension & OPEB Plans](#)].

## Changes

We inquired with Kennesy Cavanah, Statewide Accountant, on May 13, 2024 about any significant updates or changes to the pension balances reported for ACFR. She noted that legislature passed House Bill 1336 in 2023 that directly affects the Volunteer Fire Fighters and Reserve Officers' Relief and Pension Plan (VFF). Legislature split the plan to comply with federal requirements set by the Internal Revenue Service. See [Washington State Legislature](#). Although the plans are separate, they are still overseen by the Board of Volunteer Firefighters (BVFF) and exist in the volunteer firefighters' and reserve officers' system as in prior years. The plan was separated into the following:

- A new plan to include only reserve law enforcement officers

- The existing plan to include only volunteer firefighters and emergency medical technicians (EMTs).

We also noted that in FY23, the Office of the State Actuary changed the Higher Education's Supplemental Retirement Plans (SRP) valuation date from June 30th to January 1st. Kennesy confirmed that the SRP valuation date will continue to be January 1 in FY24 and future years. We confirmed the valuation date of January 1 would still meet requirements set by the Governmental Accounting Standards Board (GASB) statement No. 68, *Accounting and Financial Reporting for Pensions*. Specifically GASB 68 states "If a valuation is not performed as of the measurement date, the total pension liability is required to be based on update procedures to roll forward amounts from an earlier actuarial valuation (performed as of a date no more than 30 months and 1 day prior to the employer's most recent year-end)." ***No issues noted.***

## **(3) Updates to Significant Account Matrix:**

We identified no updates to the Significant Account Matrix based on our understanding of the line item.

## **I.4.PR.G - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset**

*Procedure Step:* Controls - Allocation of Pension Amounts

*Prepared By:* BM2, 5/28/2024

*Reviewed By:* RKM, 7/5/2024



# State of Washington

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls.

**Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

## State of Washington

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- Initiation:* How are transactions initiated?
- Authorization:* How are transactions and accounting record maintenance authorized?
- Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general,

## State of Washington

it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

Internal controls in the manual pension calculations address the following balance(s):

Statement of Net Position - Government Wide	Statement of Net Position - Proprietary Funds	Various financial statements
Deferred Outflows of Resources (Pension)	Deferred Outflows of Resources (Pension)	Deferred Outflows on Pensions
Restricted Net Pension Asset	Restricted Net Pension Asset	Restricted Net Pension Asset
Long-Term Liabilities Due in More than One Year (Net Pension Liability)	Net Pension Liability (Noncurrent)	Net Pension Liability (Noncurrent)
Deferred Inflows of Resources (Pension)	Deferred Inflows of Resources (Pension)	Deferred Inflows of Resources (Pension)

# State of Washington

For the following assertions:

## **Valuation**

There is a risk that balances (e.g. deferred outflows of resources, deferred inflows of resources, pension assets, pension liabilities) related to pension have not been measured in accordance with GASB Statement No. 68.

There is a risk the actuary uses inappropriate assumptions or actuarial methods that are not in conformity with GASB Statement No. 68 and the Actuarial Standards of Practice, causing errors in the computation of pension balances.

There is a risk the amounts included in the schedule of employer allocations and schedule of pension amounts prepared by the plan specific to the employer, including the employer amount used in the allocation percentage (that is, the numerator of the calculation), are not accurate.

There is a risk the employer-specific deferred inflows and outflows of resources (including contributions made after the measurement date, changes in proportion, and differences between the employer's actual contributions and its proportionate share of total employer contributions) have not been properly measured in accordance with GASB Statement No. 68.

There is a risk that employer's proportionate share of the pension amounts (e.g. deferred outflows of resources, deferred inflows of resources, pension assets, pension liabilities, pension expense) is not consistent with the manner in which the employer's contributions are made to the plan.

## **Completeness**

Census data reported by the employer to the plan is not accurate and complete

## **Classification**

There is a risk that the allocation between funds is not representative of the agencies included in that roll-up fund

## **General Risk (Reliance on Specialist)**

There is a risk the plan auditor's report and accompanying schedule of employer allocations and schedule of pension amounts are not adequate or appropriate for the employer auditor's purposes (for example, opinion modification, opinion on the schedule as a whole and not the individual elements, employer or employer auditor, or both, not named in the report as a specified user).

There is a risk the plan auditor engaged to report on the schedule of employer allocations and schedule of pension amounts does not have the necessary competence and objectivity for the employer auditor's purposes.

## **Gain an Understanding of Internal Controls**

We met with Kenney Cavanah, Statewide Accountant, on May 13, 2024 to gain an understanding of controls related to pension balances reported for the ACFR.

# State of Washington

## DATA VALIDATION

The FY2024 ACFR utilizes the FY2023 Department of Retirement System (DRS) Participating Employer Financial Information (PEFI) report in determining pension amounts for DRS administered Cost sharing Multiple-Employer, Defined Benefit Plans (Plan 1&2 types)/Hybrid Benefit Plans (Plan 3 types). The Office of the State Actuary certifies the DRS schedule of collective pension amounts that is included within the PEFI. The PEFI schedules are also audited by an independent auditor, Uhy. We perform a review of UHY workpapers to determine if we can place reliance on their work in the ACFR. As part of our review, we consider UHY's work performed specifically on the PEFI. For FY23 (FY23 PEFI is used to prepare FY23 statements), we noted the following: "Based on the auditors planning, work performed over census data, and substantive procedures, we determined sufficient procedures were performed to address risks. We noted conclusions made at the workpaper level agreed with the auditors' opinions. We determined sufficient procedures were performed over census data, the allocation basis, and allocation percentages. We determined we can rely on the auditors work over the PEFI." See prior year work in S1Washington-FS23, J.4 "Work of Other Audits - DRS." ***No issues noted.***

Employer contribution transmittals DRS received and processed within the fiscal year ended June 30, 2023, are used as the basis for determining each employer's proportionate share of the collective pension amounts reported in the Schedule of Employer and Non-employer Allocations for all plans - except LEOFF Plan 1, which is fully funded and no further employer contributions have been required since June 2000. OFM conducts comparisons of DRS data to HRMS data to verify the PEFI report's contribution data for completeness and accuracy.

The Human Resource Management System (HRMS) does not contain detailed employer contribution data for Higher Education and Department of Transportation (DOT). Kennesy Cavanah, Statewide Accountant, informed us that Higher education entities and DOT report summary information. Therefore, it is necessary to have these agencies provide the breakdown by plan. Differences between DRS and AFRS data causes differences in JV workbook totals; therefore, OFM sends query results to the entities requiring allocation information by plan and a reconciliation of DRS and AFRS amounts with variances explained. Higher Ed and DOT perform their own testing to verify accuracy of DRS data and certify amounts to OFM. The calculations are not final until after the Higher Education disclosures are submitted and certified. After OFM approves the contribution data from Higher Education and DOT, their data then can be included in the employer contribution totals used in the DRS allocation percentage for each plan and provided the allocation for governmental funds as a whole and each proprietary roll-up fund **(Key Control 1 - Completeness and Valuation)**.

OFM conducts a "high-level" comparison of total employer contributions by plan from DRS to HRMS. It is expected that variances will be identified in the high-level comparison due to the cash vs. accrual queries and plan management fees recorded in HRMS, but not included in DRS amounts. OFM staff perform analytical tests on employer contribution amounts in HRMS by reconciling detailed data to DRS system reports. Specifically, they reconcile the following:

- agency employer contribution amounts in HRMS to DRS employer contributions
- DRS employer contributions summary to the DRS employer contribution on the DRS e-services reports
- DRS employer contributions summary and e-services report to the DRS Schedule of Employer Allocations

# State of Washington

In August of 2023 the FY2023 DRS data was available to OFM. The FY2023 data is used for the FY2024 ACFR. Kennesy Cavanah, Statewide Accountant, performed the comparison noted above in preparation of the FY2024 ACFR **(Key Control 2 - Completeness and Valuation)**.

## **ALLOCATION OF AMOUNTS**

The allocation process does not begin until OFM receives the Higher Education institutions completed disclosures that give their pensions amounts. Kennesy said these disclosures are completed and available typically around September and OFM has no issues completing the allocation process within the ACFR JV submission timeline. OFM has created separate JV reconciliation workbooks for each plan, however, the methodology is essentially the same for all plan types. Kennesy informed us that the FY2024 allocation process will be the same allocation process that was done in the FY2023 ACFR. We will remain aware of any significant changes throughout the completion of this audit.

The allocation of DRS plan pension amounts for the state is prepared using the following steps:

- Total balances per plan are obtained from the DRS PEFI's Schedule of Collective Pension Amounts (includes net pension liability/asset, components of deferred inflows/outflows, and pension expense/income)

- The total employer contributions for the plan is obtained from DRS disclosure form (validated by OFM, see data validation above)

- The State's proportionate share of pension amounts are obtained from DRS PEFI's Schedule of Employer and Nonemployer Allocations

- OFM determines the state's proportionate share of all pension amounts for each plan (collective pension amounts and contribution disclosure amounts multiplied by the State's proportionate share), this is summarized in each plan's workbook in the "Schedule of Pension Amounts" tab

## **How Transactions are Recorded in AFRS:**

### Journal Entries:

AFRS pension balances are calculated with OFM spreadsheets that are created for each plan type. Kennesy Cavanah, Statewide Accountant, prepares the OFM spreadsheets using the DRS PEFI figures and employer contributions to calculate and record pension balances for each plan type by roll-up fund **(Key Control #3 - Completeness, Valuation, Classification)**.

For reporting in the ACFR, the state's total proportionate share of pension amounts is further allocated by a group of sort codes (rollup fund, agency, and statement code). To prepare the allocation of pension amounts for ACFR reporting, Kennesy performs the following:

- OFM obtains detailed employer contribution information from HRMS, DOT, and Higher Eds (validated by OFM, see data validation above)

- Employer contribution reports pulled from HRMS/received by DOT and Higher Eds include the agency, fund, retirement plan, and employer contributions.

- OFM uses the ACFR database in Access to assign agencies to their appropriate rollup fund, fund type, and statement code. This is done by merging the employer contribution reports and D53 agency function table in Access.

- When a new agency is created, OFM will update the tables in the ACFR Database to assign the appropriate rollup fund, and function

- OFM groups employer contributions (from the ACFR database report) by rollup fund, fund type, and statement code in each plan's spreadsheet tab "Allocation Rollup-Function"

## State of Washington

The sum for each rollup fund group is divided by the total employer contributions to determine the rollup fund allocation percentage. OFM allocates the state's proportionate share of all pension amounts by rollup fund allocation percentage (State proportionate share x rollup fund allocation percentage) in the "Schedule of Pension Amounts" tab.

The calculated pension expense, deferred outflows, deferred inflows, net pension liabilities and assets for each plan are summarized in the "JV Summary" tab by rollup fund/function. Kennessy uses calculated amounts from the "JV Summary" tab to prepare journal entries to record all components of the pension balances. The JV's are reviewed and approved by Sara Rupe, Deputy Statewide Accounting Director, and then reviewed/released by another statewide accountant separate from the pension reconciliation process.

Kennessy also runs an Enterprise Report, summarizing the GL balances for all plans after the JVs are posted to ensure amounts are accurate. Since JVs are not posted until year end, we reviewed the prior year's enterprise report and confirmed JV amounts recorded in AFRS are accurate.

### Key Controls are as Follows:

**Key Control #1 (Manual)** - Higher Ed and DOT certify to OFM that they have verified, in all material aspects, the employer amounts (employer contributions) used in the DRS allocation percentage for each plan and provided the allocation for governmental funds as a whole and each proprietary roll-up fund (**Completeness, Valuation**).

**Key Control #2 (Manual)** - OFM performs a reconciliation of agency employer contribution amounts in HRMS to DRS employer contributions, DRS employer contributions summary to the DRS employer contribution on the DRS e services reports, and DRS employer contributions summary and e-services report to the DRS Schedule of Employer Allocations (**Completeness, Valuation**).

**Key Control #3 (Manual)** - Kennessy Cavanah, Statewide Accountant, prepares the OFM spreadsheets using the DRS PEFI figures and employer contributions to calculate and record pension balances for each plan type by roll-up fund (**Completeness, Valuation, Classification**).

### Noted Weaknesses are as Follows:

None.

### I.4.PR.G - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset

*Procedure Step:* Key Control 1 (Manual)

*Prepared By:* BM2, 5/23/2024

*Reviewed By:* RKM, 7/5/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm if Higher Ed and DOT certify to OFM that they have verified, in all material aspects, the employer amounts (employer contributions) used in the DRS allocation percentage for each plan and provided the allocation for governmental funds as a whole and each proprietary roll-up fund (**key control 1 for Allocation of Pension Amounts**) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent



## State of Washington

material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. *Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. *Controls are not related to a "significant risk" identified in the audit plan.*

## State of Washington

*C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 1 (Valuation and Completeness):** Higher Ed and DOT certify to OFM that they have verified, in all material aspects, the employer amounts (employer contributions) used in the DRS allocation percentage for each plan and provided the allocation for governmental funds as a whole and each proprietary roll-up fund.

The understanding for this system is documented above in the "Controls - Allocation of Pension Amounts" step.

### **1. Confirmation of Key Manual Control:**

We obtained the Department of Transportation (DOT) certified spreadsheet that will be used for the FY2024 ACFR from Kennesy Cavanah, Statewide Accountant, on May 22, 2024. The file was titled "DOT\_FY23."

We reviewed the spreadsheet and noted the FY2023 data was on the "Summary" tab, which is the information used for the FY2024 ACFR. On the "Summary" tab we confirmed the department entered all required information into the yellow highlighted cells as directed. This process is the same for Higher education employer contribution data.

There was a .6% variance of \$(394,553) and DOT explained the variance is due to a difference in cash vs accrual methods and Agency 410 & 411 not being in the HRMS total. Kennesy confirmed that these variances happen with DOT year to year and their explanation is valid given the variance size. We also noted that the HRMS vs AFRS and HRMS vs DRS amounts accounted for the total variance of DOT. On the bottom of the

## State of Washington

spreadsheet, OFM had the statement "By submitting this spreadsheet, the Department of Transportation certifies to OFM that they have verified, in all material aspects, the FY2023 employer amounts (employer contributions) used in the DRS allocation percentage for each plan and provided the allocation for governmental funds as a whole and each proprietary roll-up fund". ***No issues noted.***

### **Noted Weaknesses are as follows:**

None.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.4.PRG - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset**

*Procedure Step:* Key Control 2 (Manual)

*Prepared By:* BM2, 5/22/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion.\*

#### **Purpose:**

To confirm OFM performs a reconciliation of agency employer contribution amounts in HRMS to DRS employer contributions, DRS employer contributions summary to the DRS employer contribution on the DRS e services reports, and DRS employer contributions summary and e-services report to the DRS Schedule of Employer Allocations (**key control 2 for Allocation of Pension Amounts**) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

# State of Washington

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control 2 (Valuation and Completeness):** OFM performs a reconciliation of agency employer contribution amounts in HRMS to DRS employer contributions, DRS employer contributions summary to the DRS employer contribution on the DRS e services reports, and DRS employer contributions summary and e-services report to the DRS Schedule of Employer Allocations.

The understanding for this system is documented above in the "Controls - Allocation of Pension Amounts" step.

### **1. Confirmation of Key Manual Control:**

We obtained the DRS to HRMS comparison spreadsheet that will be used for the FY2024 ACFR from Kennesy Cavanah, Statewide Accountant, on May 21, 2024. The file was titled "DRS\_vs\_HRMS\_Data\_Comparison\_2024"

We noted that OFM compared \$ and % differences between FY2024 HRMS and DRS data for employer contributions. The spreadsheet included any difference between the two data sets as well as any follow up procedures for variances. OFM determined they would only follow up on any significant variances (+/- \$10,000 and +/-5%).

We reviewed the data comparison and identified one agency that met the criteria for follow up, Student Achievement Council. The agency had a difference of \$(62,242.23) and -6.89%. Based on Kennesy's review of the identified variance, she confirmed that "the majority of the difference is due to the TIAA-CREF amount in HRMS, but not in DRS." The explanation is reasonable and we confirmed this agrees with prior year ACFR workpapers. We noted that no other agencies had any differences near the 10% threshold and all agencies (other than DOT or HigherEd) that had a +/- \$10,000 differences had explanations to not follow up for being a low percentage. The overall total difference for the DRS to HRMS comparison was **(\$107,898.47), .97%** of the total DRS employer contributions. **No issues noted.**

### **Noted Weaknesses are as follows:**

None.

### **2. Preliminary Control Risk Assessment**

## State of Washington

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

#### **I.4.PRG - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset**

*Procedure Step:* Key Control 3 (Manual)

*Prepared By:* BM2, 5/21/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm OFM prepares spreadsheets to calculate and record pension balances for each plan type (**key control 3 for Allocation of Pension Amounts**) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries,*

## State of Washington

*inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*



## State of Washington

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 3 (Valuation, Completeness, and Classification):** Kennesy Cavanah, Statewide Accountant, prepares the OFM spreadsheets using the DRS PEFI figures and employer contributions to calculate and record pension balances for each plan type by roll-up fund.

# State of Washington

The understanding for this system is documented above in the "Controls - Allocation of Pension Amounts" step.

## **1. Confirmation of Key Manual Control:**

We obtained OFM's pension balance calculation workbook related to PERS 1 for ACFR fiscal year 2023 (titled "PERS1\_JV\_Worksheet\_and\_Reconciliation") from Kennesy Cavanah, Statewide Accountant, on May 13, 2024. Since the fiscal year 2024 pension amounts and workbooks are not expected to be completed until after phase 2 close (September 2024) and no significant changes were made with the allocation process, we determined review of the prior year workbooks would provide sufficient coverage to confirm the control.

We identified the following key tabs used in calculating pension balances for PERS 1:

- Pension Disclosure Form (FY22 and FY21) - This is a summary of covered payroll, employer contributions, member contributions, and state contributions for each plan. The total employer contributions are used in calculations on the schedule of pension amounts.

- Allocation Rollup-Function (FY22 and FY21) - To determine allocations by fund and agency functions. This is used to calculate the pension amounts for ACFR reporting and changes in proportion for FY2023.

- DRS Allocation (FY22 and FY21) - To determine the state's proportionate share for the plan based on PEFI.

- Schedule of Pension Amounts (FY22 and FY21) - Calculation of pension amounts based on state's proportionate share (obtained from PEFI) and further by rollup/agency function allocation percentage.

- JV Summary - Summarizes JV entry using T accounts for the total state pension amounts. The entry is made based on these amounts.

- Rollup Function Summary tabs for each (999 700A, 999 700B, 999 700C, etc.) - Summarizes JV entry using T accounts for each rollup fund/agency function. Breaks them out separately for review and detail purposes.

To confirm that OFM calculated pension amounts accurately and recorded them properly, we reviewed the

"PERS1\_JV\_Worksheet\_and\_Reconciliation" and verified figures used in the calculation were accurate and supported.

- FY22 State Proportionate Share - OFM used 42.181026% as the allocation percentage for the State of Washington in their calculations. We vouched the allocation percentage to DRS' PEFI for 2022. The state's allocation percentage for PERS 1 was .453420% and 41.727606% for UAAL (Total of 42.181026%).

- Collective pension amounts - OFM used collective pension amounts from DRS' PEFI for 2022 to determine the state's proportionate share. We vouched the net pension liability (\$2,784,367,000) from the "Schedule of Pension Amounts" tab to PEFI, along with the deferred inflow/outflow components and pension expense. All amounts used in calculation tied to source documents (PEFI) without exception.

- State's Share of Net Pension Liability - OFM calculated the State's proportionate share of net pension liability for PERS 1 to be \$1,174,474,568 (\$2.8 billion \* 42.18%). Calculation appears accurate. We traced this amount to the notes to the financial statements (Note 15, Retirement Plans) for FY23 with no exception.

We selected one rollup fund/agency function allocation to trace from calculation to entry, rollup fund 999 and agency function 700A.

The allocation percentage for the selected rollup fund/agency function was 7.16% based on employer contributions of \$18.4 million divided by total employer contributions of \$257.8 million. Calculation appears accurate.

# State of Washington

The ending net pension liability was \$84,036,610 ( $\$2,784,367,000 * 42.181026\% * 7.16\%$ )

The ending net pension liability per the JV summary agreed to the amount calculated in the "Schedule of Pension Amounts" tab. We reviewed JVOFM036 to ensure the entry was accurate, all amounts agreed to the t account from the JV summary and calculations. JVOFM036 was prepared by Kenesey Cavanah, Statewide Accountant, on April 27, 2023 and reviewed and approved by Sara Rupe, Deputy Statewide Accounting Director, on May 1, 2024. ***No issues noted.***

## Noted Weaknesses are as follows:

None.

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.4.PR.G - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset**

*Procedure Step:* Risk Assessment

*Prepared By:* BM2, 8/13/2024

*Reviewed By:* RKM, 8/22/2024

Purpose/Conclusion.\*

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy.\*

Auditors are **required** to perform the following procedures for each line item:

# State of Washington

## **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

# State of Washington

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

## **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk*

## State of Washington

*of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

**Completeness - High**

**Valuation - High**

**Classification - High**

### **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

#### **GASB Allocation of Pension Amounts**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**Completeness - High**

# State of Washington

**Valuation - High**

**Classification - High**

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

### **Substantive Test: DRS Administered Pension Plans**

Step 1: Determine the type of pension plans the employer participates in. See full list of state plans identified at [[Pension & OPEB Plans](#)].

Step 2: Use the applicable GASB 68 Testing Spreadsheet to re-recalculate the reported pension balances from the PEFI report

Step 3: Special Funding Situation: Ensure employers are recognizing pension expense and an equal amount of revenue for their share of contributions to the LEOFF 2 plan, made on their behalf by the state

Step 4: Test allocation of pension amounts to funds and activities (as applicable)

Step 5: Review Required Supplementary Information (RSI)

Step 6: Review note disclosures for accuracy and completeness

We will follow the testing strategy for GASB 68 at [[Substantive Test: DRS Administered Pension Plans](#)]

### **Substantive Test: Supplemental Retirement Plans**

Step 1: Tie Financial Statement Amounts to Actuary Report

Step 2: Review note disclosures for accuracy and completeness

Step 3: Review Required Supplementary Information

We will follow the testing strategy for GASB 68 at [[Substantive Test: Supplemental Retirement Plans](#)].

### **Rely on the work of a Specialist**

We will follow the testing strategy in order to rely on the work of a specialist for GASB 68 [[Rely on Specialist \(DRS Plans\)](#)] and [[Rely on Specialist \(SRP\)](#)].

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

## **I.4.PRG - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset**

*Procedure Step:* Substantive Test: DRS Administered Pension Plans

# State of Washington

*Prepared By:* MRF, 11/14/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

**Purpose:**

To confirm pension balances and disclosures are correctly reported.

**Conclusion:**

We determined:

- Pension balances are correctly valued and classified
- Pension disclosures are accurate and complete
- Pension RSI schedules are accurate and complete

**No issues noted**

Testing Strategy:

Before auditing this area auditors should obtain an appropriate understanding:

Review [BARS Manual part 3.4.2](#) BARS GAAP Manual – Accounting – Liabilities – Pensions

Consider the following additional steps:

Accounting/Auditing self-study training

[GASB 68 Pensions - Year 2](#)

[Pension and OPEB Reporting from the Auditors' and Actuaries' Experience](#)

Scan the DRS Employer [website](#) for GASB 68 resources

Participating Employer Financial Information (PEFI)

eServices Contribution Reconciliation

*As detailed in the Guidance/Criteria tab of this audit step:*

*Additional rely on specialist procedures and management representations are not required.*

*Some employers report to DRS under more than one employer ID number, these employers should combine all PEFI amounts for financial statement reporting; our workpaper has this factored in (there is no additional adjustment necessary)*

*Volunteer Fire Fighters and Reserve Officers Retirement System (VFFRPF) if applicable is expected to be immaterial. If disclosed in the notes and reported as a net pension asset consider tying amounts to client supporting documentation.*

To determine whether pensions were properly reported, auditors are **required** to perform the following procedures:



# State of Washington

## **STEP 1 for all plans: Determine the type of pension plan(s) in which the employer participated in FY2023**

**Defined Contribution plans:** The following information should be disclosed in notes to the financial statements about each defined contribution pension plan to which the **employer contributes** to the plan. If only employees contribute, then the employer is not a participant and no disclosures are required.

Name of pension plan, identification of the public employee retirement system or other administrative entity, and that it is a defined contribution pension plan

Brief description of benefit terms (including any terms related to vesting and forfeitures and the policy related to the use of forfeited amounts) and authority under which benefit terms are established or may be amended

Contribution (or crediting) rates (in dollars or as a percentage of salary) for employees, employer, and any non-employer contributing entities, and the authority under which those rates are established or may be amended

Amount of pension expense recognized by the employer in the reporting period

Amount of forfeitures reflected in pension expense recognized by the employer in the reporting period

Amount of the employer's liability outstanding at the end of the period, if any.

There are no pension liabilities (except for any outstanding payable due for contributions) or deferred outflows/inflows to report. *No further work is necessary for Defined Contribution plans.*

### **Defined Benefit plans:**

Single-employer plans:

Governmental & Proprietary Governments

The cities of Seattle, Spokane and Tacoma have their own pension plans in addition to participation in the closed LEOFF 1 plan. A number of cities, counties and some fire districts have obligations remaining from police and firefighter plans in existence before state plans were established (sometimes referred to as "pre-LEOFF 1" plans). These are closed plans with no active members. Auditors should check for existence of these plans and expect such a plan for any governments who receive Fire Insurance Premium tax (BARS 336.06.91), which are listed as an Appendix in the Pension / OPEB planning guide. Contact a Pension / OPEB Subject Matter Expert if a government is receiving this funding but does not have a plan or to alert the specialist to any previously unidentified single-employer plans.

Proprietary Only

4-year and community colleges report a Supplemental Retirement Plan, that pension is covered by its own testing strategy.

If other single employer plans are identified where the government administers its own defined benefit pension plan, contact the Pension/OPEB Subject Matter Experts.

Non-governmental defined benefit pension plans – Some local governments may provide pensions to their employees through a cost-sharing, multiple-employer defined benefit pension plan that is not a state or local governmental pension plan. For example, a union sponsored plan.

## State of Washington

Participating employers do not report a pension liability, deferred outflows or deferred inflows in their financial statements. Pension expense is equal to the employer's required contributions to the plan. See the BARS manual for note disclosure and RSI requirements.

*Continue with the testing strategy to review reporting and disclosure requirements for Defined Benefit plans.*

### STEP 2: Obtain GASB 68 Workpaper and employer contributions

Obtain the appropriate GASB 68 workpaper from the TeamStore which is based off 1) the year-end of the government and 2) the measurement date of the relied upon actuary report.

*The earliest measurement date that can be used by an employer is 12 months earlier than the reporting date.*

Earliest Available Valuation Date	Earliest Available Measurement Date Employer Can Use	Employer Reporting Date
6/30/2019	6/30/2020	6/30/2021
6/30/2020	6/30/2021	8/31/2021
6/30/2020	6/30/2021	12/31/2021

*Therefore, local governments with a reporting date of 6/30/21 can use **either** the 6/30/20 **or** 6/30/21 schedules for their year-end balances. Due to timing of the publication of the PEFI reports most local governments with a 6/30/21 year end elected to use the 6/30/20 report. Local governments with a reporting date of 12/31/21 should use the 6/30/21 schedules for their year-end balances.*

On the INPUT tab, follow the instructions to enter the Organization ID Number (obtained from the 20XX\_PEFI tab) and Employer's FYE.

Request from the client pension contributions subsequent to the measurement date up through the employer's reporting date, and enter on INPUT tab.

*Contribution amounts should be actual employer contributions, on the accrual basis, to each plan. For PERS 1 (and TERS 1) this includes PERS 2/3 and PSERS 2 "Plan 1 UAAL" contributions (and TERS 2/3 and SERS). Plan 1 UAAL contributions are Plan 1 contributions, not Plan 2 contributions. Employers should have supporting documentation obtained from the DRS eServices contributions system to support all contribution amounts.*

All state pension plans tested by this procedure are identified on the GAAP-Summary tab.

### STEP 3: Compare expected pensions amounts to reported

## State of Washington

Use the GAAP-Summary tab to compare reported amounts per client to expected for the following financial statement amounts:

Net Pension Asset/Liability

*No expected current portion/due within one year for net pension liabilities as those amounts are paid with plan assets.*

Deferred Outflows/Inflows

Pension Expense (a component of payroll expense)

*Employers should have supporting documentation of their calculations for audit. If amounts per auditor calculations do not agree to employer amounts, use the individual plan summary tabs to research and identify errors. The individual plan tabs are the same tool provided to local governments in the BARS Manual.*

*In addition to the collective deferred outflows and deferred inflows reported in the PEFI for each plan, employers must also recognize their own employer-specific DO/DI. Test the mathematical accuracy of the following:*

*Employer contributions made subsequent to the measurement date of the net pension liability/(asset), but before the end of the employer's fiscal year – recognized as a deferred outflow.*

*Change in Proportionate Share – The net effect of changes in the allocation percentage between years - recognized as of the beginning of the period. A table to calculate the change in proportionate share is included on each plan tab in the attached spreadsheet. An additional table to calculate amortization of current and prior year changes in proportionate share is also included on each plan spreadsheet.*

If net pension assets exist, see BARS [3.4.2.63](#) for how **restricted net position** should be reported and disclosed. Recalculating restricted net position is not required, however auditors will need to confirm what method was applied (and disclosed). If no restricted net position was reported then should calculate the error using SAO's preferred method.

### **Step 4: Special Funding Situation: Ensure employers are recognizing pension expense and an equal amount of revenue for their share of contributions to the LEOFF 2 plan, made on their behalf by the state**

LEOFF plans 1 and 2 include a special funding situation in which the State has a legal obligation to make contributions directly to the plans.

Although the State makes the contributions, individual employers are required to recognize pension expense and an equal amount of revenue for their share of these contributions.

LEOFF 1 is fully funded and there have been no contributions since 2000. No further action (other than note disclosure) is currently necessary.

LEOFF 2 – The total amount contributed by the State appears at the end of the LEOFF 2 Employer Allocation Schedule in the PEFI. Note that allocation percentages have not been calculated for individual employers and each individual employer must calculate their own share of the State's total contributions.

Formula: See the "SpecFndg" tab in the attached spreadsheet. This spreadsheet explains the calculation of the special funding amount, the required journal entry, and note disclosures.

# State of Washington

Verify that employers have recorded this transaction.

## **STEP 5: Test allocation of pension amounts to funds and activities (as applicable)**

For GAAP statements that include multiple opinion units, pension liabilities/(assets), deferred outflows and deferred inflows should be allocated between governmental and business-type activities in the government-wide statement of net position, allocated to appropriate activities in the government-wide statement of activities, and reported in the specific proprietary or fiduciary funds they are directly related to and expected to be paid from.

Auditors should evaluate allocations for reasonableness by:

- Understanding and evaluating the reasonableness of the allocation methodology. We expect the methodology to be consistent from year to year.

- Testing the mathematical accuracy of formulas used and tracing amounts to the financial statements.

- SAO recommends the effect of changes in allocation percentages from year to year be expensed in the current year. However, employers may amortize these changes over the remaining service life of the plan if they choose.

## **STEP 6: Review Required Supplementary Information (RSI)**

Inquire with management about the methods of preparing the schedules, including:

- Whether it is measured and presented in accordance with GAAP

- Whether methods of measurement or presentation have been changed from those used in the prior period and the reasons for any such changes.

- Whether there were any significant assumptions or interpretations underlying the measurement or presentation of the information.

Verify that RSI is included with all and only the required elements

*See the BARS Manual for [State sponsored pension plans](#) (PERS, PSERS, LEOFF).*

Read the schedule for consistency with inquiry and knowledge obtained during the audit.

Foot and cross-foot schedules and tie key figures reported in the schedule to the financial statements, notes and underlying accounting records.

*Note that the Schedule of Proportionate Share of the Net Pension Liability is dated as of the measurement date of the plans (e.g. 6/30 for*

## State of Washington

*state sponsored plans) and the Schedule of Employer Contributions is dated as of the employer's reporting date (e.g. 12/31 for most local governments). When these two dates are different, we expect the amount reported for covered payroll to be different on the two schedules. "Covered payroll" is the payroll on which contributions to a pension plan are based. For PERS 1 (and TERS 1), covered payroll includes not only the payroll related to active plan 1 employees, but also the payroll from PERS 2/3 and PSERS (or TERS 2/3 and SERS) because these plans determine plan 1 UAAL contributions. "Contributions" are actual employer contributions into the plans. For plan 1's, this includes plan 2 contributions that fund the plan 1 UAAL's.*

Consider additional work as necessary to address any risks noted.

### **STEP 7: Review note disclosures for accuracy and completeness**

Compare disclosures to the BARS manual template notes for state sponsored plans.

*Local governments may, but are not required to, use this sample note disclosure. The sample note meets the minimum disclosure requirements of GASB 68 and local governments may include additional information as considered necessary for a fair and accurate presentation. The attached spreadsheet includes sample DO/DI and amortization tables for the notes on each plan spreadsheet.*

Foot and cross-foot schedules and tie key figures reported in the notes to the financial statements, PEFI report, underlying accounting records, and other sources, as necessary.

If net pension assets exist the notes should disclose the method used to calculate restricted net position. All significant accounting policies require disclosure (either under note 1 or along with the pension note).

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

For assistance contact Pension/OPEB subject matter experts.

### **Pension and OPEB Planning Guide**

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

## State of Washington

**AICPA Audit Guide for State and Local Governments – [Chapter 13](#) Defined Benefit Pension Plans**

### **GASB Codification sections P20–P24**

Record of Work Done:

#### **STEP 1 for all plans: Determine the type of pension plan(s) in which the employer participates**

The significant retirement plans administered by DRS that are subject to audit are listed here [[Pension & OPEB Plans](#)].

#### **STEP 2: Use GASB 68 Testing Spreadsheet to re-calculate reported pension balances from the Participating Employer Financial Information (PEFI) report. (Completeness)**

We used the auditor pension tool to test the mathematical accuracy of the calculation of the net pension liability (and/or asset), deferred outflows and deferred inflows amounts reported by the employer for each plan using the Schedules of Collective Pension Amounts in the PEFI.

The teamstore workpaper recalculates each employer's proportionate share of pension balances for state-sponsored plans using PEFI data, however, does not calculate amounts for the total state. We made the following modifications to the pension confirmation workbook available in the teamstore:

In all PEFI tabs (source: Data provided by DRS directly to SAO), we summarized employer contributions by plan for ONLY state of washington. We obtained State of Washington figures for employer contributions and allocation percentage (from the applicable PEFI) and included the information in PEFI tabs. For 2023 PEFI, this included:

PERS1	N/A	State of Washington - Employer Allocations	2,197,031.60	0.322414%	State of Washington
PERS1	N/A	State of Washington - Plan 1 UAAL	288,539,875.15	42.343117%	State of Washington
PERS23	N/A	State of Washington - Employer Allocations	449,409,550.99	51.114528%	State of Washington
PSERS	N/A	State of Washington - Employer Allocations	33,198,299.77	65.933914%	State of Washington
TRS1	N/A	State of Washington - Employer Allocations	109,560.56	0.020299%	State of Washington
TRS1	N/A	State of Washington - Plan 1 UAAL	7,687,443.72	1.424334%	State of Washington

## State of Washington

TRS23	N/A	State of Washington - Employer Allocations	9,633,439.82	1.423660%	State of Washington
LEOFF2	N/A	State of Washington - Employer Allocations	1,634,912.94	0.724320%	State of Washington

We assigned an ORG ID of N/A for the total State of Washington PEFI amounts to allow for formulas to calculate by using the ORG ID N/A in the input tab.

Calculation changes made for employers related to special funding contributions are not applicable to State of Washington, see Step 4 below. We removed the special funding calculation from the "GAAP-Summary" tab.

We hid SERS calculations from "GAAP-Summary" and SERS tabs as the State of Washington made no contributions to this plan and therefore had no allocation of liabilities.

**See** [[Pension confirmation \(GASB 68\) – DRS plans 12-31-23](#)].

### STEP 3: Compare expected pensions amounts to reported (Valuation)

We used the GAAP-Summary tab from modified Team Store Workpaper to compare reported amounts per client to expected for the following financial statement amounts:

Net Pension Asset/Liability

*No expected current portion/due within one year for net pension liabilities as those amounts are paid with plan assets. **No issues noted***

Deferred Outflows/Inflows **No issues noted**

Pension Expense (a component of payroll expense). **No issues noted.**

In addition to the collective deferred outflows and deferred inflows reported in the PEFI for each plan, employers must also recognize their own employer-specific DO/DI. We tested the mathematical accuracy of the following:

*Employer contributions made subsequent to the measurement date of the net pension liability/(asset), but before the end of the employer's fiscal year – recognized as a deferred outflow. **No issues noted***

*Change in Proportionate Share – The net effect of changes in the allocation percentage between years - recognized as of the beginning of the period. A table to calculate the change in proportionate share is included on each plan tab in the attached spreadsheet. An additional table to calculate amortization of current and prior year changes in proportionate share is also included on each plan spreadsheet. **No issues noted***

**Step 4: Special Funding Situation: Ensure employers are recognizing pension expense and an equal amount of revenue for their share of contributions to the LEOFF 2 plan, made on their behalf by the state.**

## State of Washington

For the State ACFR, the special funding contribution to the LEOFF 2 plan made by the state for the benefit of other municipalities (outside of its own employer contributions for agencies that participate in the plan) is entirely an expense of the state. Adjustments to the special funding tab removes the calculation of other municipalities' proportionate share of the state's special funding contribution, i.e. the special funding is 100% state expense. See the "SpecFndg" tab in [[Pension confirmation \(GASB 68\) – DRS plans 12-31-23](#)] spreadsheet.

### **STEP 5: Test allocation of pension amounts to funds and activities (as applicable)**

For GAAP statements that include multiple opinion units, pension liabilities/(assets), deferred outflows and deferred inflows should be allocated between governmental and business-type activities in the government-wide statement of net position, allocated to appropriate activities in the government-wide statement of activities, and reported in the specific proprietary or fiduciary funds they are directly related to and expected to be paid from.

Auditors should evaluate allocations for reasonableness by:

- Understanding and evaluating the reasonableness of the allocation methodology. We expect the methodology to be consistent from year to year.

- Testing the mathematical accuracy of formulas used and tracing amounts to the financial statements.

We reviewed the OFM workbooks for each of the plans, and the specific fund tabs. We reviewed the T-accounts used to calculate the deferred inflows and outflows, and noted the adjustments complied with GASB 68 standards.

We confirmed that the total allocated for all funds within a pension plan, was equal to the amount allocated to the pension plan as a whole with the state's proportionate share. As we traced fund allocations we reviewed the fund function to determine if the agencies reporting to that fund are reasonable based on the agency type.

We recalculated the allocation among opinion units here [[Line Item Lead Sheet](#)]. I.4.1 tab "Fund Breakdown" Using OFM workbooks to recalculate the total pension asset (liability) for each fund based on DRS total amount, and OFM calculated allocation. This amount is tested in I.4.6 [[Pension confirmation \(GASB 68\) – DRS plans 12-31-23](#)]. We determined we can rely on the allocation percentages. Each pension plan gets reported in different funds. OFM performs a calculation based on contributions to each fund, and determines a percentage for each fund of the total plan contributions.

The "fund" tab of OFM's workbook has the following actions for each fund code in each pension plan:

- Reverse the prior year deferred outflows. Deferred Outflows of PY are recognized in the current period as a decrease by crediting the PY recorded amount.

- Reverse the prior year's deferred inflows. Deferred inflows of PY are recognized in the current period as an decrease by debiting the PY recorded amount.

- Include the current year's pension expense. This is the pension expense as allocated by the FY23 Proportional Share

- Include the current year's deferred inflows (if any). Again, total balance is tracked and reported by DRS, and OFM allocates to the funds with the proportional share, then fund share percentages.

- Include deferred outflows, all contributions made to the plan after the measurement date close (end of previous fiscal year)



# State of Washington

On the "AFRS Balance to Rollup Fund" tab, we compared the OFM reported total as traced in testing (Fund Breakdown tab), to the amount reported in AFRS (ACFR Queries tab). All variances noted were below the floor, and we will not carry them to the AOM. **No issues noted.**

## **STEP 6: Review Required Supplementary Information (RSI)**

See [2024 ACFR RSI - Pension Plans]. Work is documented here [RSI: Pension Plan Information].

## **STEP 7: Review note disclosures for accuracy and completeness**

See [Note 15: Retirement Plans]. Work is documented here [Note 15: Retirement Plans].

### I.4.PRG - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset

*Procedure Step:* Substantive Test: Supplemental Retirement Plans

*Prepared By:* MRF, 11/14/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm that the Higher Education Supplemental Retirement Plan pension balances and disclosures are correctly reported.

#### **Conclusion:**

We determined state pension plan:

Balances are correctly valued and classified/allocated correctly

Disclosures are accurate and complete

RSI schedules are accurate and complete

Testing Strategy:

### **Step 1: Tie Financial Statement Amounts to Actuary Report**

**a) Tie the following financial statement figures to the actuary report:**

# State of Washington

## **Net Pension Liability Pension Expense Deferred Inflows Deferred Outflows**

*The financial statement pension balances will include non-SRP activity — to test only the portion of the balance related to the SRP, auditors should document what GL accounts they're testing (or by testing to the related journal entry).*

*Pension expense is not discretely presented on the change statement as it is a component of employee benefits. Typically, the colleges should be making monthly benefit payments and contributions to the plan – these amounts are recorded throughout the year as pension expense. The remaining expected pension expense is posted at year-end using information from the actuary report.*

### **b) Recalculate the current/noncurrent portion of the Net Pension Liability:**

*SRP benefit funds are currently restricted from paying SRP benefits and are not expected to pay benefits until approximately 2035. Until this time, SRP benefit payments are paid by the colleges on a pay-as-you-go basis, meaning employers pay these benefits as they occur. As a result, colleges should report a current portion due. The current portion is required by GASB 34, ¶31.*

### **Step 2: Review note disclosures for accuracy and completeness**

#### **Trace key figures in the notes to the actuary report (or roll-forward)**

*Document work or use tick-marks to demonstrate note figures tie to actuary report. Expected note tables include:*

*Development of the Net Pension Liability*

*Sensitivity of the Net Pension Liability to Changes in the Discount Rate*

*Deferred Resources*

*5-year recognition (and thereafter) table of DO/DI*

*Employees Covered by the Benefit Terms (only updated by OSA for the new valuation, not the roll-forward). Using prior year data for this disclosure is a trivial error.*

### **Step 3: Review Required Supplementary Information**

Inquire with management about the methods of preparing the schedules, including:

Whether it is measured and presented in accordance with GAAP

Whether methods of measurement or presentation have been changed from those used in the prior period and the reasons for any such changes.

# State of Washington

Whether there were any significant assumptions or interpretations underlying the measurement or presentation of the information.

Verify that RSI is included with all and only the required elements

## **RSI – Schedule of Changes in the Net Pension Liability and Related Ratios**

**Confirm key figures in the RSI to the actuary report**

## **RSI – Schedule of Employer Contributions**

**Confirm key figures in the RSI to the actuary report and accounting records**

Guidance/Criteria.:

Record of Work Done.:

### **Step 1: Tie Financial Statement Amounts to Actuary Report**

We obtained the 2024 Higher Education Supplemental Retirement Plan information in the workbook *2024 GASB Results - Final*, which was accompanied by the SRP.Actuarial.Certification.Letter [[SRP.Actuarial.Certification.Letter](#)]. This information was provided to OFM, and forwarded to SAO via email. The 2024 report was not posted on the OSA website as of 11/08/2024. See actuary report here [[2024 GASB Results - Final - From OSA](#)]

We reviewed the spreadsheet created by OFM to determine whether the OSA 2023 Actuarial Valuation change from June 30th to January 1st for Higher Education SRPs will affect the State's ability to remain within GASB 68 Net Pension Liability reporting compliance. We determined that the valuation date will not affect the State's ability to remain within compliance of GASB 68 reporting requirement of having a Net Pension Liability valuation within 30 months and 1 day of the fiscal year-end. See here [[HigherEdSup\\_Proposed\\_Val\\_Measure\\_Report\\_Dates](#)]. No issues noted.

a) Tied the following financial statement figures to the actuary report [[SRP Confirmations to Actuary Report](#)] :

- Net Pension Liability
- Pension Expense
- Deferred Inflows
- Deferred Outflows

## State of Washington

The allocation methodology among functions and funds for the SRP pension line amounts are similar to the DRS administered plans as described in [\[Controls - Allocation of Pension Amounts\]](#) except specifically for employer contributions, based upon fund type, to the HE SRP and allocated proportionately to the roll-up funds. We recalculated the allocated amounts [\[Line Item Lead Sheet\]](#) (Fund Breakdown tab) and tied the post-allocated amounts of the SRP amounts to the financial statements at [\[Line Item Lead Sheet\]](#) (AFRS Balance to Rollup Fund tab) with no exceptions.  
**No issues noted.**

### **Step 2: Review Note Disclosures for Accuracy and Completeness**

See [\[Note 15: Retirement Plans\]](#).

### **Step 3: Review Required Supplementary Information**

See [\[2024 ACFR RSI - Pension Plans\]](#).

### **I.4.PR.G - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset**

*Procedure Step:* Rely on Specialist (DRS Plans)  
*Prepared By:* BM2, 10/24/2024  
*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

#### **Purpose:**

To determine if we can rely on the work of Office of the State Actuary to provide audit evidence for liabilities for DRS sponsored pension plans.

#### **Conclusion:**

We determined that we **can** rely on the work of the specialist.

Testing Strategy:

To determine whether the audit can rely on the work of the outside specialist and whether the specialist's work supports the financial statements, the following procedures are **required** to be performed:

## State of Washington

Auditor should check with their supervisor whenever they determine that the use of a specialist may be necessary.

*A specialist is an individual or organization possessing expertise in a field other than accounting or auditing (for example, information technology specialists, engineers and actuaries). Specialists may be contracted or employed by entity management to assist them in performing their responsibilities (management's specialist) or contracted or employed by our Office (auditor's specialist).*

*This step does not need to be completed when consulting with attorney general assistants, LGS, TAS, LISA, STAT, DSI or "Subject Matter Experts" designated on the intranet. Contact TAS for assistance if needed to determine whether someone would be considered a specialist or not.*

Assess the specialist's competence, capability and objectivity as it relates to the work that we intend to rely on for the audit.

*Competence refers to the specialist's relevant qualifications and experience. In assessing competence, auditors should consider:*

*The education, professional certifications or licenses of the specialist in his or her field, as appropriate.*

*The reputation and standing of the specialist.*

*The specialist's experience in the type of work under consideration.*

*Our Office's experience in using the specialist's work, if applicable.*

*Capability refers to effect of any access, resource or other limitations on the specialist's work. In assessing capability, auditors should consider:*

*Timing of the specialists work*

*Any significant limitations on the specialist's access to needed information or people*

*Any significant limitations on the time the specialist was able to devote to the work*

*Our Office's experience in using the specialist's work, if applicable.*

*Objectivity refers to the possible effects of any bias, conflicts of interest or undue influence on the specialist's judgment. If the specialist's objectivity is impaired, the auditor may not rely on the work of the specialist. In assessing objectivity, auditors should consider:*

*Any pressures or incentives on either specialists or management to misstate*

## State of Washington

*Threats to objectivity of the specialist (including self-interest, advocacy, familiarity, self-review or intimidation threats) and any safeguards in place (segregation of duties, lines of reporting, professional standards, formality and consistency of methods and assumptions, retrospective reviews, etc)*

*Our Office's experience in using the specialist's work, if applicable.*

*Auditors should contact TAS if the auditor has any concerns with assessing the competence, capabilities or objectivity of specialists.*

Obtain an understanding of the work and conclusions of the specialist. This understanding should include the following elements:

- Objectives and scope of the specialist's work
- Intended use of the specialist's work to support the audit objective
- Specialist procedures and conclusions
- Assumptions and methods used by the specialist

*The objectives and scope of the specialists work and intended use of the specialist's work to support our audit objective should have already been included in the audit plan or else will need to be documented as a change to the audit plan.*

Evaluate the work and conclusions of the specialist. This evaluation should include the following elements as applicable:

Relevance and reasonableness of the specialist's methods and assumptions

*The appropriateness and reasonableness of methods and assumptions used and their application are the responsibility of the specialist. However, if the auditor concludes that the specialist's findings are unreasonable in the circumstances, the auditor should apply alternative procedures, which may include obtaining the opinion of another specialist.*

*Auditors should specifically consider whether methods and assumptions changed from the preceding period and the reasons for such changes, if applicable.*

Appropriate tests of source data provided by the entity to the specialist.

*If any data used by the specialist was provided by the entity, the auditor should consider the risk that incomplete or inaccurate data may materially affect the specialist's conclusions. This risk may be affected by the auditor's assessment of overall COSO elements and control risk for the related system.*

*For example: when relying on work of an actuary for self-insurance liabilities, auditors would normally verify the completeness and accuracy of claims information provided to the actuary against claims information per the pool's system. This can be done by*

## State of Washington

*comparing the total claim payments per pool's records to total claims paid shown on the actuary reports (in aggregate or on annual basis) – the figures may not match exactly but should be very close.*

Relevance and reasonableness of the specialist's conclusions.

Verifying that the specialist's conclusions are reflected in the financial statements

Add an additional representation to the rep letter if the specialist used was employed or contracted by management (rather than SAO). See the List of Additional Representations located in the Auditor Reference Guide here: [Representation Letter Resource.docx](#)

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [3230](#) - Using the Work of Specialists**

Record of Work Done:

### **Assessment of Competence, Capabilities and Objectivity of Specialist**

We assessed the competence, capabilities and objectivity of the specialist, specifically considering factors described in the testing strategy.

#### **1. Competence**

Two individuals certified the 2023 Participating Employer Financial Information (PEFI) report [[2023 PEFI Actuarial Certification Letter](#)]:

*Matthew M. Smith, FCA, EA, MAAA, State Actuary (Signatory on Actuarial Valuation, DRS ACFR and PEFI Actuarial Certification Letter)*

Matt has been with the Office of the State Actuary for 22 years (November 2002)

Matthew M. Smith is a Fellow of the Conference of Consulting Actuaries (FCA) since 2005, an Enrolled Actuary (EA) since 1999, and a member of the American Academy of Actuaries (MAAA) since 1999.

Matt is Washington's third State Actuary and serves as executive head of OSA. As the State Actuary, Matt oversees the annual actuarial valuations of 14 public retirement plans. He directs the actuarial services for the state's prepaid tuition program, certain medical programs, and the Long-Term Services and Supports Trust Program. OSA also provides staff and assistance to the Select Committee on Pension Policy (SCPP), a 20-member statutory committee. The SCPP studies issues and policies affecting the Washington State Retirement Systems and makes recommendations to the Legislature. Matt directs research and policy staff in support of the SCPP.

*Michael T. Harbour, ASA, MAAA, Actuary (Prepared Actuarial Estimate)*

Michael has been with the Office of the State Actuary for 17 years (2007)

## State of Washington

He is an associate of the Society of Actuaries (ASA) since 2017 and a member of the American Academy of Actuaries (MAAA) since 2017

We verified their credentials by reviewing the [actuarial directory](#) (hosted by both SOA and AAA) and verified their standings as members of both organizations. We noted that they were both compliant with SOA Continuing Professional Development requirements. ***No issues noted.***

### 2. Capability

Capability relates to the ability of the specialist to exercise their competence. The Office of the State Actuary works exclusively on the funding and benefit issues of Washington State's Retirement System. There were no limitations on the specialist's access to needed information or people and time the specialist was able to devote to the work. They have worked closely with State agencies in the past. Based on our Office's past experiences, we determined they are capable of performing their actuarial duties. We have been able to rely on their work in the past without issues. We believe they continue to be capable and we can rely on their reports.

Based on review of the report criteria, completeness of the information through reconciliation of systems and census data noted in [[Key Control 2 \(Manual\)](#)], as well as lack of pressure or incentive for specialists to misstate, we determined we can rely on the capabilities of the specialist to perform the work. ***No issues noted.***

### 3. Objectivity

The Office of the State Actuary is an independent and non-partisan agency of the Washington State Legislature and works primarily on the funding and benefit issues of the state's public retirement systems. The Office was created in 1977 and its duties are set forth in RCW [44.44](#) and [41.24.320](#). The role of the Office as currently defined is to:

- Prepare actuarial valuations of all DRS plans, including studies required by law.
- Provide fiscal notes/all pension legislation.
- Advise Legislature/Governor on pension issues.
- Staff the Select Committee on Pension Policy.
- Provide actuarial assistance to: Department of Retirement Systems & LEOFF 2 Retirement Board, committee on advanced tuition payment, long term services and supports trust commission, and Employment Security Department related to the family and medical leave program.

We noted no evidence to indicate pressures or incentives on specialists to misstate. Threats to objectivity of the specialist or lack of safeguards were not noted. There was no indication that information was withheld from the specialist by the DRS or related entities. Based on their independence, we determined we can rely on the objectivity of the specialist. ***No issues noted.***

### **Understanding of Specialist's Work and Conclusions**

We gained an understanding of the specialist's procedures and conclusions, including the methods and assumptions used, and noted the following:



# State of Washington

## **1. Objectives and scope of the specialist's work**

The primary purpose of the information provided by the OSA, is to satisfy the actuarial reporting requirements of GASB. Actuarial valuations of the plans are used by the Office of the State Actuary (OSA) in determining the funded status and funding progress of the plans. The State Actuary's Office performs all actuarial services for the State sponsored plans, including all studies required by law. This includes conducting valuations of the separate systems. The valuations are presented in the Actuarial Valuations Report available on the State Actuary's website: [Office of the State Actuary](#). The report is located in Valuations under the Pension Funding menu on the site's home page.

For further detail of the specialist's work, see the 2023 ACFR Actuarial Certification Letter at [\[2023 ACFR Actuarial Certification Letter\]](#) and the 2023 PEFI Certification Letter here at [\[2023 PEFI Actuarial Certification Letter\]](#). *No issues noted.*

## **2. Intended use of the specialist's work to support the audit objective**

OSA calculates the total pension liability for each plan. OSA also calculates the amortization schedules for the deferred inflows and outflows, and the pension expense that are recorded in the Schedules of Collective Pension Amounts. We will review the actuarial valuation to ensure that assumptions and methodologies were reasonable for calculation of pension balances.

## **3. Specialist procedures and conclusions**

OSA receives member and beneficiaries information from the Department of Retirement Systems (DRS). Assets and financial information are provided by the Washington State Investment Board (WSIB) and DRS. Employer contribution transmittals DRS received and processed within the fiscal year ended June 30, 2023, are used as the basis for determining each employer's proportionate share of the collective pension amounts reported in the Schedule of Employer and Non-employer Allocations for all plans. LEOFF Plan 1 is fully funded and no further employer contributions have been required since June 2000. The latest Actuarial Valuation was performed as of August 2024, which is within 30 months and 1 day prior to DRS' year-end/measurement date, June 30, 2023, as required by GASB 68. See [\[2023 DRS Plans Actuarial Valuation\]](#). *No issues noted.*

## **4. Assumptions and methods used by the specialist**

To calculate the contribution rates necessary to pre-fund the plan's benefits, an actuary uses an actuarial cost method, asset valuation method, funding policy economic assumptions, and demographic assumptions. The Entry Age Normal (EAN) cost method is used to report the plans' funded status. The annual cost of benefits under EAN is comprised of two components: normal cost, plus amortization of the unfunded liability. The normal cost is most commonly determined on an individual basis, from a member's age at plan entry, and is designed to be a level percentage of pay throughout a member's career. Comparing the EAN liabilities to the actuarial value of assets on the valuation date provides an appropriate measure of a plan's funded status and is acceptable according to current Governmental Accounting Standards Board (GASB) Statements 67 and 68.

The plan's assets were used to calculate contribution rates, unfunded liabilities, and the plan's funded status. Because the market value of assets

## State of Washington

can be volatile from one year to the next, an asset valuation method is generally used to adjust the market value of assets and smooth the effects of short-term volatility. The adjusted assets are called the actuarial value of assets, or valuation assets. In the valuation process, assumptions are required for four economic variables; expected investment rate of return, inflation, general salary growth and membership growth. Economic assumptions affect expectations regarding the accumulation of assets and the growth of projected pension benefits. The Pension Funding Council (PFC) adopts economic assumptions for all plans/systems except LEOFF 2. The LEOFF 2 Board adopts economic assumptions for LEOFF 2. All economic assumptions are then subject to revision by the Legislature. Demographic assumptions include, but are not limited to, rates of retirement, probability of termination, rates at which members become disabled, turnover rates, mortality rates.

In the State Actuary's opinion, all methods, assumptions, and calculations are reasonable and are in conformity with generally accepted actuarial principles and standards of practice as of the date of the June 30, 2023 Actuarial Report (dated August 2024). All methods and assumptions can be found on the [State Actuary's Website](#). In addition, in the State Actuary's opinion, the PEFI disclosures were prepared in accordance with GASB Statement 68. **See Actuarial Certification Letter for the PEFI at [2023 PEFI Actuarial Certification Letter]**. NOTE: The valuations were used to determine the criteria Actuaries used in their assumptions for the PEFI and ACFR. The amounts reviewed for State ACFR items came from the PEFI for multi-employer plans and from the ACFR for single employer plans. *No issues noted.*

Changes for the 2023 valuation include:

- No changes to economic or demographic assumptions since the prior valuation.

- Adjustments to methods for calculating UAAL contribution rates in PERS 1 and TRS 1 to reflect the delay between the measurement date of calculated Plan 1 rates and when the rates are collected.

- Adjustments to OSA's model to reflect past inflation experience when modeling future COLAs for current annuitants in all plans except PERS 1 and TRS 1

### **Evaluation of Specialist's Work**

#### **1. Relevance and Reasonableness of the Specialist's Methods and Assumptions**

We reviewed the methods and assumptions used in determining the total pension liability to ensure they are in accordance with GASB Statement No. 68 and Actuarial Standards of Practice. We noted that 12 of 16 DRS plans [[Pension & OPEB Plans](#)] are cost sharing multiple employer defined benefit plans. Key actuarial requirements under [GASB Statement No. 68](#) (for cost-sharing multiple employer defined benefit plans, paragraphs 48-71) include:

- Paragraph 60: Pension liability should be determined by an actuarial valuation as of the measurement date or the use of update procedures to roll forward to the measurement date amounts from an actuarial valuation as of a date no more than 30 months and 1 day earlier than the employer's most recent fiscal year end.

- Paragraph 60: For accounting and financial reporting purposes, an actuarial valuation of the pension liability should be performed at least biennially.

- Paragraph 61: Unless otherwise specified by the Statement, the selection of all assumptions used in determining the pension liability and related measures should be made in conformity with Actuarial Standards of Practice issued by the Actuarial Standards Board.

## State of Washington

Paragraph 62: Projected benefit payments should include all benefits to be provided to current active and inactive employees through the pension plan in accordance with the benefit terms and any additional legal agreements to provide benefits that are in force at the measurement date.

Paragraph 62: Projected benefit payments should include the effects of automatic postemployment benefit changes, including automatic COLAs

Paragraph 64: The discount rate should be the single rate that reflects:

The long-term expected rate of return on pension plan investments that are expected to be used to finance the payment of benefits, to the extent that (1) the pension plan's fiduciary net position is projected (in conformity with [paragraphs 65–67](#)) to be sufficient to make projected benefit payments (determined in conformity with [paragraphs 62](#) and [63](#)) and (2) pension plan assets are expected to be invested using a strategy to achieve that return

A yield or index rate for 20-year, tax-exempt general obligation municipal bonds with an average rating of AA/Aa or higher (or equivalent quality on another rating scale), to the extent that the conditions in (a) are not met.

Paragraph 70: The entry age actuarial cost method should be used to attribute the actuarial present value of projected benefit payments of each employee to periods in conformity with the following:

Attribution should be made on an individual employee-by-employee basis.

Each employee's service costs should be level as a percentage of that employee's projected pay. For purposes of this calculation, if an employee does not have projected pay, the projected inflation rate should be used in place of the projected rate of change in salary.

The beginning of the attribution period should be the first period in which the employee's service accrues pensions under the benefit terms, notwithstanding vesting or other similar terms.

The service costs of all pensions should be attributed through all assumed exit ages, through retirement. In pension plans in which the benefit terms include a DROP, for purposes of this Statement, the date of entry into the DROP should be considered to be the employee's retirement date.

Each employee's service costs should be determined based on the same benefit terms reflected in that employee's actuarial present value of projected benefit payments.

We reviewed the Washington State 2023 Actuarial Valuation Report and determined that the specialist's methods and assumptions are relevant and reasonable. Methods and assumptions used by OSA are in accordance with key actuarial requirements from GASB 68. We also noted in the State Actuary's opinion, all methods, assumptions, and calculations are reasonable and are in conformity with generally accepted actuarial principles and standards of practice as of the date of the June 30, 2023 Actuarial Report (dated August 2024). ***No issues noted.***

### **2. Appropriate tests of source data provided by the entity to the specialist**

Office of the State Actuary obtains audited member and beneficiary data from the Department of Retirement Systems (DRS). DRS contracts with Uhy LLP to audit the PEFI and ACFR. As part of the PEFI audit, Uhy reviews employer contributions that allocation percentages are based on. As part of the ACFR audit, Uhy LLP reviews active and inactive membership (headcount and census data). Uhy LLP provided an unmodified opinion

## State of Washington

for both ACFR and PEFI. We perform a CPA review of Uhy LLP's audit of DRS' ACFR and PEFI. We reviewed audit workpapers related to June 30, 2023 DRS ACFR and PEFI as part of the prior year ACFR audit, S1Washington-FS23 in folder J.4. We noted the following:

### *PEFI Census Data testing:*

*UHY performed targeted sampling at each employer through utilization of comprehensive data analysis for the full population of the employer payroll records. Application of the analysis and sampling is detailed below.*

*Eligibility Analysis: The full population of each employer's payroll file was cross referenced against DRS census in order to identify those who were excluded from the census. A dollar value threshold for fiscal year wages was established for sampling purposes through which eligibility and participation would have been likely. Employees with wages over this threshold were selected to assess whether their exclusion from participation, as well as census, was appropriate. A sample of up to 10 employees was selected from the group that was flagged through their analysis.*

*Date of Birth Analysis: The full population of each employer's payroll file was cross referenced against the employer's comprehensive employee information report. The date of birth for every employee in the employer's fiscal year 2022 payroll was tested against the census allowing for full coverage of the population. For all instances in which the date of birth per the employee information report did not match the census, each was selected for testing. The auditor obtained official government issued IDs or official tax and employment forms in order to determine the correct date of birth.*

*Service Credit Calculation: The full population of each employer's payroll file was cross referenced against DRS census to identify all individuals on both the payroll and census. Based on key employment dates (hire, leave, termination), the auditor calculated the estimated months of service credit. For instances in which the estimated service credit did not agree within 12 months, a sample up to 10 employees was selected for detailed testing. For each selection, the auditor obtained detailed employment records and incorporated service credit earned from prior employment.*

*Compensation Analysis: The full population of each employer's fiscal year 2022 payroll file were summed by employee, with consideration for the eligibility of wages when the data was available. Employee wages were matched against the census and the differences were stratified by amount. A sample of up to 10 employees was selected with selections focused on instances in which the wages, per the employer's payroll records, differed from the census by more than \$5,000. For each selection, the auditor obtained employee paystubs including a detailed breakdown of the wages to assess eligibility. Additionally, wages from prior employment were obtained to aid in reconciling to the census.*

*The auditor noted that based on their audit procedures they have concluded that there was no significant impact on the actuarial valuation or net pension liability of the Washington State Department of Retirement Systems resulting from the census data testing. Their audit provided reasonable assurance that the financial statements are free from material misstatement.*

### *PEFI Contribution testing:*

*Confirmations*

## State of Washington

*The auditors determined confirmations were the most effective method of testing contributions and obtaining adequate coverage. 25 contribution confirmations were sent, and all were received. We reviewed the control confirmation log at 7500.00. We also reviewed the results of the confirmations (confirmation reconciliation). No significant exceptions were noted. We noted contribution confirmations were recalculated. The auditors noted recalculation of allocations tied within an immaterial variance (\$28,946 or .00015%).*

*Analytical Procedures (7006.01)*

*We reviewed a substantive contribution analytical. Employer and employee contributions were considered in the analytical. Recalculated contributions were within expectations. Reconciliation of Contributions Reported on the PEFI to the DRS ACFR (7003 and 7004). We reviewed the reconciliation of PEFI contributions to the DRS ACFR. We noted amounts tied without exception*

OSA also checks the data for reasonableness based on the purpose of their valuation. ***No issues noted.***

### **3. Relevance and reasonableness of the specialist's conclusions**

We reviewed the 2023 DRS ACFR and the 2023 PEFI Actuarial Valuation Certification letters for valuation dates of June 30, 2023. **See: [2023 PEFI Actuarial Certification Letter] & [2023 ACFR Actuarial Certification Letter]. *No issues noted.***

#### 2023 ACFR (DRS)

OSA performed the most recent actuarial valuation in 2023 with a valuation date of June 30, 2022. The total pension liability was calculated as of the valuation date and projected to the measurement date of June 30, 2023. Plan liabilities were rolled forward from June 30, 2022, to June 30, 2023, reflecting each plan's normal cost (using the Entry Age cost method), assumed interest, and actual benefit payments. GASB 67 requires an "asset sufficiency test" to determine whether (or how long) OSA can use the long-term expected rate of return on assets to measure the present value of accrued plan liabilities for accounting purposes. See the entire documented actuarial valuation process for the 2023 ACFR at [2023 ACFR Actuarial Certification Letter]. ***No issues noted.***

#### 2023 PEFI (2023)

OSA prepared the following information for inclusion in the 2023 Participating Employer Financial Information (PEFI):

Schedules of Collective Pension Amounts, Fiscal Year 2023  
Amortization Schedules and Pension Expense under Note 2

We believe the data, methods, and assumptions used in the actuary's valuation process/procedure are reasonable and appropriate. Based on our review, we determined that the specialist's conclusions are relevant and reasonable. ***No issues noted.***

### **4. Verifying that the specialist's conclusions are reflected in the financial statements**

See substantive tests performed at [Substantive Test: DRS Administered Pension Plans].

## State of Washington

### 5. If the specialist used was employed or contracted by management, add an additional representation to the Management Representation Letter related to the work of the specialist.

We added a representation related to the use of an actuary, see [\[Concluding\]](#).

#### I.4.PRG - Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset

*Procedure Step:* Rely on Specialist (SRP)

*Prepared By:* MRF, 11/18/2024

*Reviewed By:* RKM, 11/21/2024

Purpose/Conclusion:

#### **Purpose:**

To determine if we can rely on the work of Office of the State Actuary to provide audit evidence for Supplementary Retirement Plan (SRP) actuariality determined values.

#### **Conclusion:**

We determined that we **can** rely on the work of the specialist.

Testing Strategy:

To determine whether the audit can rely on the work of the outside specialist and whether the specialist's work supports the financial statements, the following procedures are **required** to be performed:

Auditor should check with their supervisor whenever they determine that the use of a specialist may be necessary.

*A specialist is an individual or organization possessing expertise in a field other than accounting or auditing (for example, information technology specialists, engineers and actuaries). Specialists may be contracted or employed by entity management to assist them in performing their responsibilities (management's specialist) or contracted or employed by our Office (auditor's specialist).*

*This step does not need to be completed when consulting with attorney general assistants, LGS, TAS, LISA, STAT, DSI or "Subject Matter*

## State of Washington

*Experts” designated on the intranet. Contact TAS for assistance if needed to determine whether someone would be considered a specialist or not.*

Assess the specialist’s competence, capability and objectivity as it relates to the work that we intend to rely on for the audit.  
*Competence refers to the specialist’s relevant qualifications and experience. In assessing competence, auditors should consider:*

*The education, professional certifications or licenses of the specialist in his or her field, as appropriate.*

*The reputation and standing of the specialist.*

*The specialist’s experience in the type of work under consideration.*

*Our Office’s experience in using the specialist’s work, if applicable.*

*Capability refers to effect of any access, resource or other limitations on the specialist’s work. In assessing capability, auditors should consider:*

*Timing of the specialists work*

*Any significant limitations on the specialist’s access to needed information or people*

*Any significant limitations on the time the specialist was able to devote to the work*

*Our Office’s experience in using the specialist’s work, if applicable.*

*Objectivity refers to the possible effects of any bias, conflicts of interest or undue influence on the specialist’s judgment. If the specialist’s objectivity is impaired, the auditor may not rely on the work of the specialist. In assessing objectivity, auditors should consider:*

*Any pressures or incentives on either specialists or management to misstate*

*Threats to objectivity of the specialist (including self-interest, advocacy, familiarity, self-review or intimidation threats) and any safeguards in place (segregation of duties, lines of reporting, professional standards, formality and consistency of methods and assumptions, retrospective reviews, etc)*

*Our Office’s experience in using the specialist’s work, if applicable.*

*Auditors should contact TAS if the auditor has any concerns with assessing the competence, capabilities or objectivity of specialists.*

Obtain an understanding of the work and conclusions of the specialist. This understanding should include the following elements:

- Objectives and scope of the specialist’s work

## State of Washington

- Intended use of the specialist's work to support the audit objective
- Specialist procedures and conclusions
- Assumptions and methods used by the specialist

*The objectives and scope of the specialists work and intended use of the specialist's work to support our audit objective should have already been included in the audit plan or else will need to be documented as a change to the audit plan.*

Evaluate the work and conclusions of the specialist. This evaluation should include the following elements as applicable:

Relevance and reasonableness of the specialist's methods and assumptions

*The appropriateness and reasonableness of methods and assumptions used and their application are the responsibility of the specialist. However, if the auditor concludes that the specialist's findings are unreasonable in the circumstances, the auditor should apply alternative procedures, which may include obtaining the opinion of another specialist.*

*Auditors should specifically consider whether methods and assumptions changed from the preceding period and the reasons for such changes, if applicable.*

Appropriate tests of source data provided by the entity to the specialist.

*If any data used by the specialist was provided by the entity, the auditor should consider the risk that incomplete or inaccurate data may materially affect the specialist's conclusions. This risk may be affected by the auditor's assessment of overall COSO elements and control risk for the related system.*

*For example: when relying on work of an actuary for self-insurance liabilities, auditors would normally verify the completeness and accuracy of claims information provided to the actuary against claims information per the pool's system. This can be done by comparing the total claim payments per pool's records to total claims paid shown on the actuary reports (in aggregate or on annual basis) – the figures may not match exactly but should be very close.*

Relevance and reasonableness of the specialist's conclusions.

Verifying that the specialist's conclusions are reflected in the financial statements

Add an additional representation to the rep letter if the specialist used was employed or contracted by management (rather than SAO). See the List of Additional Representations located in the Auditor Reference Guide here: [Representation Letter Resource.docx](#)



# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **SAO Audit Policy [3230](#) - Using the Work of Specialists**

Record of Work Done:

## **Assessment of Competence, Capabilities and Objectivity of Specialist**

We assessed the competence, capabilities and objectivity of the specialist, specifically considering factors described in the testing strategy.

### **1. Competence**

Two individuals certified the 2024 Supplemental Retirement Plan Valuation for Higher Education: Lisa Won, Deputy State Actuary, and Michael Harbour, Actuary, certified the 2024 Actuarial Valuation report.

Lisa Won, ASA, FCA, and MAAA - Deputy State Actuary. Lisa has been with OSA since 2007 and has been Deputy State Actuary since 2016. She received an undergraduate degree in Actuarial Science from the University of Waterloo in Ontario Canada. Lisa is an associate of the Society of Actuaries (ASA), a Fellow of the Conference of Consulting Actuaries (FCA), and a member of the American Academy of Actuaries (MAAA). To become an FCA, the candidate must be engaged in actuarial work as a consultant, in government, as an insurance employee or as an Enrolled Agent. One prerequisite has the candidate obtaining six years of actuarial experience and hold the ASA, ACAS, EA, MAAA or MSPA designation. As the Deputy State Actuary, Lisa oversees the annual actuarial valuations of 14 public retirement plans. OSA also provides staff and assistance to the Select Committee on Pension Policy (SCPP), a 20-member statutory committee. The SCPP studies issues and policies affecting the Washington State Retirement Systems and makes recommendations to the Legislature. Lisa contributes direction for research and policy staff in support of the SCPP. **No issues noted.**

*Michael Harbour, ASA, MAAA- Actuarial Analyst (Prepared Actuarial Estimate)*-Michael has been with OSA since 2007. He is an associate of the Society of Actuaries (ASA) and a member of the American Academy of Actuaries (MAAA). **No issues noted.**

We verified that Lisa Won's and Michael Harbour's credentials were in good standing with the American Academy of Actuaries at [actuary.org](http://actuary.org), and Conference of Consulting Actuaries at [ccactuaries.org](http://ccactuaries.org).

SAO has worked with Lisa and Michael as actuaries in the past. Our office has always had a good experience using the specialist's work for the GASB 68 Census Data Examination that we performed for the Department of Retirement Systems in prior years. Based on the qualification,

# State of Washington

experience, and credentials of the individual noted above, we determined that we can rely on the competence of the specialists. ***No issues noted.***

## **2. Capability**

Capability relates to the ability of the specialist to exercise their competence. The Office of the State Actuary works exclusively on the funding and benefit issues of Washington State's Retirement System. They have worked closely with State agencies in the past. Based on our Office's past experiences, we determined they are capable of performing their actuarial duties. We have been able to rely on their work in the past without issues. We believe they continue to be capable and we can rely on their reports.

Based on review of the report criteria, completeness of the information, as well as lack of pressure or incentive for specialists to misstate, we determined we can rely on the capabilities of the specialist to perform the work. ***No issues noted.***

## **3. Objectivity**

The Office of the State Actuary is an independent and non-partisan agency of the Washington State Legislature and works primarily on the funding and benefit issues of the state's public retirement systems. The Office was created in 1977 and its duties are set forth in Chapters 44.44 and 41.24 RCW. The role of the Office as currently defined is to:

- Prepare actuarial valuations of the plans.
- Provide fiscal notes/all pension legislation.
- Advise Legislature/Governor on pension issues.
- Staff the Select Committee on Pension Policy.
- Provide actuarial assistance to: Department of Retirement Systems & LEOFF 2 Retirement Board

For Higher Education SRP, per RCW 28B.10.423:

Each institution of higher education that is responsible for payment of supplemental amounts shall contract with the state actuary for an actuarial valuation of their supplemental benefit plan. Each institutional shall also contract with the state actuary for actuarial experience study of the mortality, service, compensation, and other experience of the annuity or retirement income plans and into the financial condition of each system. Upon completion of the valuation or experience study, the state actuary shall provide copies of the study to the institution of higher education and to the select committee on pension policy and the pension funding council.

We noted no evidence to indicate pressures or incentives on specialists to misstate. Threats to objectivity of the specialist or lack of safeguards were not noted. There was no indication that information was withheld from the specialist by the DRS or related entities. Based on their independence from DRS, we determined we can rely on the objectivity of the specialist. ***No issues noted.***

## **Understanding of Specialist's Work and Conclusions**

# State of Washington

We gained an understanding of the specialist's procedures and conclusions, including the methods and assumptions used, and noted the following:

**1. Objectives and scope of the specialist's work** (2024 Higher Education SRP Actuarial Valuation letter [[SRP.Actuarial.Certification.Letter](#)])

The primary purpose of the valuation is to provide information to the higher education institutions in order to meet the financial reporting requirements under GASB Statement No. 67/68 for the fiscal year ending June 30, 2024.

**2. Intended use of the specialist's work to support the audit objective**

OSA calculates the total pension liability for participating entity. OSA also calculates the amortization schedules of the deferred inflows and outflows, and the pension expense that are recorded in the Schedules of Collective Pension Amounts. These are used by OFM to value the Higher Education SRP for the participating entities.

**3. Specialist procedures and conclusions**

OSA relies on participant data provided by entities and retirement plan vendors to perform the valuation. An update to the plan participant data file was provided as of January 1, 2024. OSA checked the data for reasonableness as appropriate based on the purpose of the valuation. An audit of the participant data was not performed. They relied on all the information provided as complete and accurate. In their opinion, this information is adequate and substantially complete for the purposes of the valuation.

**4. Assumptions and methods used by the specialist**

The assumptions used in the valuation, including total salary growth and the demographic assumptions, were developed in the 2023 Economic Experience Study report. OSA considered input from TIAA, a Retirement Plan vendor, to help us set the economic assumptions related to the Assumed Income. OSA determined the discount rate based upon the 2021 Economic Experience Study for the Washington State retirement plans and based on the results of the GASB 67/68 crossover test. In their opinion, all methods, assumptions, and calculations are reasonable and are in conformity with generally accepted actuarial principles and standards of practice as of the date of the letter.

To calculate the contribution rates necessary to pre-fund the plan's benefits, an actuary uses an actuarial cost method, asset valuation method, economic assumptions, and demographic assumptions. The Entry Age Normal (EAN) cost method is used to report the plans' funded status. The annual cost of benefits under EAN is comprised of two components: normal cost, plus amortization of the unfunded liability. The normal cost is most commonly determined on an individual basis, from a member's age at plan entry, and is designed to be a level percentage of pay throughout a member's career. Comparing the EAN liabilities to the actuarial value of assets on the valuation date provides an appropriate measure of a plan's funded status and is acceptable according to current Governmental Accounting Standards Board (GASB) Statements 67 and 68.

Assumptions from the previous year are generally the same.

We noted rate of return for plan assets returned to the standard 7.0%, as the discount rate to measure the Total Pension Liability (TPL).

# State of Washington

The plan's assets were used to calculate contribution rates, unfunded liabilities, and the plan's funded status. Because the market value of assets can be volatile from one year to the next, an asset valuation method is generally used to adjust the market value of assets and smooth the effects of short-term volatility. The adjusted assets are called the actuarial value of assets, or valuation assets.

In the valuation process, assumptions are required for four economic variables; expected investment rate of return, inflation, general salary growth and membership growth. Economic assumptions affect expectations regarding the accumulation of assets and the growth of projected pension benefits. The Pension Funding Council (PFC) adopts economic assumptions for the plan. All economic assumptions are then subject to revision by the Legislature.

Demographic assumptions include, but are not limited to, rates of retirement, probability of termination, rates at which members become disabled, turnover rates, mortality rates.

In the State Actuary's opinion, all methods, assumptions, and calculations are reasonable and are in conformity with generally accepted actuarial principles and standards of practice as of the date of the June 30, 2024 Actuarial Valuation Report (dated October 2024). All methods and assumptions can be found on the State Actuary's Website, see OSA Assumptions. ***No issues noted.***

## **Evaluation of Specialist's Work**

### **1. Relevance and reasonableness of the specialist's methods and assumptions.**

We reviewed the methods and assumptions used in determining the total pension liability are in accordance with GASB Statement No. 67/68 and Actuarial Standards of Practice and are the same as those used by the plan. These seem appropriate based upon our review. In the State Actuary's opinion, all methods, assumptions, and calculations are reasonable and are in conformity with generally accepted actuarial principles and standards of practice as of the date of the June 30, 2024 Actuarial Valuation Report (dated October 2024). We reviewed the Washington State 2024 Actuarial Valuation Report and determined that the specialist's methods and assumptions are relevant and reasonable. ***No issues noted.***

### **2. Appropriate tests of source data provided by the entity to the specialist.**

We obtained OFM's JV Workbooks by entity for the SRP, amortization schedules, and corresponding JV's from Kenney Cavanah, Statewide Accountant.

The Washington State Investment Board, the Office of Financial Management, and the Department of Retirement Systems provided financial and asset information as of June 30, 2024. OSA checked the participant data and assets for reasonableness as appropriate based on the purpose of the valuation. They relied on the information provided as complete and accurate. In their opinion, this information was adequate and substantially complete for the purposes of the valuation.

In order to ensure a reasonable valuation, OSA developed eligibility criteria to determine which actives (or members currently on leave) should be

## State of Washington

included in the SRP valuation. The criteria relies on the calculated First Contribution Date, the institution's SRP closure date (Plan Closure Date), and the employee's date of hire. Starting with the census files provided to us by the institutions, we relied on the following rules to determine who should be included or excluded from the valuation.

1. An active employee must be participating in the Higher Education Retirement Plan (HERP) to be eligible for a SRP benefit.
2. If an active employee has a First Contribution Date that occurs prior to the Plan Closure Date, they are included on the valuation file.
3. If an active employee has a First Contribution Date that occurs on or after the Plan Closure Date, they are included on the valuation file only if their date of hire is before the Plan Closure Date.
4. All other active employees were excluded from the valuation file. They were either reported with a date of hire and First Contribution Date that occurred on or after the Plan Closure Date or they were reported with no HERP contribution information.

### **3. Relevance and reasonableness of the specialist's conclusions.**

We reviewed the Actuarial Certification Letter along with the reports. We believe the data, methods, and assumptions used in the actuary's valuation process/procedure are reasonable and appropriate. Based on our review, we determined that the specialist's conclusions are relevant and reasonable.

### **4. Verifying that the specialist's conclusions are reflected in the financial statements.**

We verified that the specialist's conclusions are reflected in the financial statements here: [\[Substantive Test: Supplemental Retirement Plans\]](#). We tied the amounts recorded in AFRS to the financial statements in our review presentation and disclosure work here [\[Proprietary Fund Financial Statements\]](#).

### **5. If the specialist used was employed or contracted by management, add an additional representation to the Management Representation Letter related to the work of the specialist.**

We added a representation related to the use of an actuary, see [\[FS Letter of Representation\]](#).

### **I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows**

*Procedure Step:* Summary & Conclusion

*Prepared By:* BM2, 11/21/2024

*Reviewed By:* RKM, 11/29/2024

Purpose/Conclusion:
---------------------

# State of Washington

## **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

## **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

### **Information to be used as audit evidence:**

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?

## State of Washington

Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?

Is information precise enough to catch if misstatements exceeded the tolerable level?

Is information detailed enough to conclude on whether or not there were misstatements?

Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?

How did misstatements occur and how often might they occur again in the population?

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

# State of Washington

## Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

## **I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows**

*Procedure Step:* Understanding of Line Item

*Prepared By:* BM2, 5/22/2024

*Reviewed By:* RKM, 7/5/2024

## Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**



## State of Washington

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

# State of Washington

Guidance/Criteria:

Record of Work Done:

**(1) Prior Audit Exceptions:**

No prior year exceptions.

**(2) Composition & Change Analysis:**

Line Item Leadsheet: [\[Line Item Lead Sheet\]](#).

In addition to pension benefits reviewed at [\[Pensions - Long-Term Liabilities, Deferred Inflows, Deferred Outflows, Net Pension Asset\]](#), the State's Health Care Authority (HCA), administers a single employer defined benefit Other Post Employment Benefits (OPEB) plan. Per Office of the State Actuary (OSA), "OPEB are benefits provided to eligible retired employees (and their spouses) beyond those provided by their pension plans. Such benefits include medical, prescription drug, life, dental, vision, disability, and long-term care insurance. PEBB was created within the Washington State Health Care Authority (HCA) to administer all these benefits for public employees, retirees, and their families. PEBB employers provide monetary assistance, or subsidies, for medical, prescription drug, dental and vision insurance." See [\[ \]](#) for understanding of Public Employees' Benefit Board (PEBB) including the state index rate, retiree benefits, and other plan information.

The Governmental Accounting Standards Board (GASB) issued GASB Statement No. 75, *Accounting and Financial Reporting for Postemployment Benefits Other than Pensions*, in June 2015 which establishes standards for recognizing and measuring liabilities, deferred outflows of resources, deferred inflows of resources, and expense/expenditures for OPEB. GASB 75 requires employers to disclose key financial measures for the plan, including the Total OPEB Liability (TOL), OPEB expense, and benefit payments (or employer contributions). The statement requires more extensive disclosures and supplementary information than the prior reporting requirements. GASB 75 became effective for employer fiscal years beginning after June 15, 2017, and requires employers to disclose key plan measures relative to their plan members, including the Total OPEB Liability (TOL) and OPEB Expense.

For ACFR, balances reported on individual statements and opinion units are percentages of state-wide OPEB balances (deferred outflows, short-term liability, long-term liability, and deferred inflows as determined by OSA's actuarial valuations). State-wide balances are audited in S1FinancialManagement-FS24. Agencies do not report OPEB balances in AFRS, OFM prepares manual AFRS journal vouchers to record balances for all agencies by opinion unit and statement.

We met with Kenesey Cavanah, Statewide Accountant, on May 13, 2024 to inquire of any significant changes to the balance and she did not identify any. She noted there are a couple new agencies for fiscal year 2024 that will be included in the allocation calculations, but that is a common occurrence from year to year.

# State of Washington

## **(3) Updates to Significant Account Matrix:**

We identified no updates to the Significant Account Matrix based on our understanding of the line item.

## **I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows**

*Procedure Step:* Controls - Allocation of OPEB Amounts

*Prepared By:* BM2, 7/2/2024

*Reviewed By:* RKM, 7/5/2024

Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

## State of Washington

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

“Key controls” refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as “key controls”) in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

- When (or how often) is the control applied

- Who performs the control

- As needed, the experience, knowledge and attitude of the person applying the control

- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer’s criteria?

- How the key control is documented or evidenced

- If not obvious from the description, how the control prevents or timely detects and corrects misstatements

- Any exceptions or alternative processing to the normal process

- What happens when misstatements or issues are identified by the control

## State of Washington

The “transaction flow” refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **Material Balance(s) and Assertions**

Internal controls in the GASB Allocation of OPEB Amounts address the following balance(s):

## State of Washington

Statement of Net Position - Government Wide	Statement of Net Position – Proprietary Funds	Various financial statements
Deferred Outflows of Resources (OPEB)	Deferred Outflows of Resources (OPEB)	Deferred Outflows of Resources (OPEB)
Long Term Liabilities Due within One Year (Other Post Employment Benefits Obligations)	Other Long Term Liabilities - Noncurrent (Other Post Employment Benefits)	Total OPEB Liability (Current)
Long Term Liabilities Due in More Than One Year (Other Post Employment Benefits Obligations)	Total OPEB Liability (Current)	Total OPEB Liability (Noncurrent)
Deferred Inflows of Resources (OPEB)	Deferred Inflows of Resources (OPEB)	Deferred Inflows of Resources (OPEB)

For the following assertions:

### **Completeness -**

Members are inappropriately excluded from, or included in, the census data

### **Valuation**

Census data does not reconcile to (agree with) the employer's payroll and personnel records or is not properly accumulated (maintained) for active and inactive members, causing errors in the computation of deferred outflows, total OPEB liability, and/or deferred inflows

The actuary uses incomplete (missing) or incorrect census data, causing errors in the computation of total deferred outflows, total OPEB liability, and/or deferred inflows

The actuary uses inappropriate assumptions or actuarial methods that are not in conformity with GASB Statement No. 75

Deferred outflows of resources and deferred inflows of resources and OPEB expense are not properly calculated and reported in accordance with GASB Statement No. 75

### **Classification**

There is a risk that the allocation between funds is not representative of the agencies included in that roll-up fund

### **Gain an Understanding of Internal Controls**

We met with Kennesy Cavanah, Statewide Accountant, on May 13, 2024 to gain an understanding over Other Post-Employment Benefits (OPEB) balances reported in the State of Washington financial statements on May 13, 2024. We used prior year work to gain our understanding of controls because OPEB data was not expected to be complete until August. We confirmed with Kennesy that the control process from the prior

# State of Washington

year will remain the same.

## Actuarial Valuation

The Office of the State Actuary (OSA), with assistance from the Health Care Authority's actuaries (Milliman), determines all OPEB balances at the State level in their annual Actuarial Valuation. Key plan details and assumptions were as follows:

Non-qualifying trust: The Washington State plan was pay-as-you-go with a substantive plan (terms understood by employers and plan members without a formalized contract or plan document).

Discount rate: The discount rate was equal to the 20-year Municipal Bond Index. The rate used for the current measurement date, June 30, 2023, was 3.65%.

Valuation: Estimates were based on Entry Age Normal actuarial cost method.

Amortization: Changes in actuary assumptions were based on the average expected remaining service lives of all active and inactive members (nine years)

## OPEB Schedules

The Statewide Accountant prepares the following schedules to report allocation of OPEB liabilities and OPEB balances by selected state agencies and in total:

Schedule of OPEB State Agency Allocations - Lists headcount and allocation percentage (agency headcount divided by total state headcount) for each agency. Based on census data as of measurement date.

Schedule of OPEB Amounts by Agency - Allocates state balances from OSA Actuarial valuation based on agency allocation percentage. This includes Total OPEB liability, deferred outflows, deferred inflows, and OPEB expense components

Notes to OPEB Schedules - Describes the plan, participants, allocation method, actuarial assumptions.

SAO performs a separate engagement with the above OPEB Schedules. We reviewed TeamMate audit file [S1FinancialManagements-FS23] for audit procedures and results over testing census data, review of actuary assumptions, and recalculation of schedules. All balances reported in OPEB Schedules were identified as significant and audit procedures included reviewing actuary assumptions (by performing the rely on specialists steps), reviewing census data accuracy, and recalculating OPEB Schedule balances. The audit resulted in 2 exit items related to benefits eligibility at one agency and a missing note disclosure. The OFM Statewide Accountant reviews the results of the OPEB Schedule audit and census data testing to ensure the completeness and accuracy of the allocation percentages used to prepare OPEB calculations (**Key Control #1: Manual - Completeness and Valuation**).

## Allocation of OPEB Amounts

OFM Statewide Accountant uses the audited OPEB balances by state agency and further allocates each agency's liability by expenses reported in sub-object BD (Health, Life & Disability Insurance) to ensure OPEB balances are properly reported in the appropriate statement and opinion unit (**Key Control #2: Manual - Valuation, Classification**). Sub-object BD was used because of the following:

## State of Washington

The Schedule of Other Post-Employment Benefits State Agency Allocations was based on an agency's number of active employees receiving health and life benefits administered by the Public Employees Benefit Board (PEBB), Benefits were allocated on the same basis as payroll (active employees), and The employer medical contribution (EMC) was expensed through sub-object BD. The EMC was the monthly amount paid by state agencies based on the number of employees eligible to receive benefits (including employees that waived coverage). The monthly rate for plan year 2024 was \$680, based on 85% of an average of UMP's bid rate. Each state agency transferred money to the Health Care Authority (HCA) after each payroll cycle (10th and 25th), the administrator of PEBB and state employee benefits. The OFM Statewide Accountant noted some state agencies have additional expenses run through sub-object BD for additional benefits. Additional benefits were typically for life insurance or other similar insurances that were significantly paid for by the employee. The OFM Statewide Accountant noted no additional benefits that were expected to skew the allocation of benefits.

The OFM Statewide Accountant modifies the audited OPEB schedules in OFM's Excel workbook 'OPEB\_JV\_Worksheets\_2023' to determine balances reported for ACFR. Kennesy prepared a procedures document that gives a step by step of the workbook to update amounts, formulas, and allocation processes. We used the 2023 workpapers for gaining our understanding of the 2024 controls and process due to timing. OPEB workbooks were prepared in August/September. See below for the following steps:

Step #1: Obtain final version of audited OPEB schedules (Schedule of Other Post-Employment Benefits State Agency Allocations).

Step #2: Export the prior year ACFR database balances for sub-object BD totaled by agency, fund, and table sort codes by index match. See tab "21\_ACFR\_Data" in OFM's Excel workbook. The prior year BD expenses were used to match the measurement date (one year lag).

Step #3: Split agency allocation percentages from the Schedule of Other Post-Employment Benefits State Agency Allocations by fund and opinion unit based on sub-object BD totals. See tabs "21\_BD% Allocation by Agency" and "19 % charged by Rollup & Function" in OFM's Excel workbook. Agencies that reported under multiple funds were highlighted in a separate color to help preparers and reviewers ensure allocations were accurately split.

Step #4: Allocations were aggregated by opinion unit and summarized in a pivot table by rollup fund, posting agency, and total. The total for the opinion unit was multiplied by the total OPEB line item balance. See tab "22 Schedule of OPEB amounts" for allocation of all audited OPEB line items in OFM's Excel workbook.

### **How transactions are recorded in AFRS:**

Kennesy Cavanah, OFM Statewide Accountant, prepares a year-end journal voucher to record the long-term liabilities balance using the actuary report and allocation schedule calculations. The calculations from OPEB\_JV\_Worksheets\_2023 Excel workbook was the support used for all OPEB JV's in AFRS. Another Statewide Accountant performs a detailed review over the OPEB excel workbook to ensure journal vouchers were supported by audited OPEB schedule amounts, accurately allocated to respective agencies and reporting funds, and accurately adjusted balances to ensure opinion units recorded state-wide balances and amounts in compliance with reporting requirements under GASB 75 (**Key Control #3: Manual - Valuation, Classification, and Completeness**). Kennesy will also verify the JV was properly posted to AFRS by running an Enterprise Reporting report and tracing amounts from the OPEB calculations to AFRS.



# State of Washington

## Key Controls are as Follows:

**Key Control #1 (Manual - Completeness and Valuation)** - The OFM Statewide Accountant reviews the results of the OPEB Schedule audit and census data testing to ensure the completeness and accuracy of the allocation percentages used to prepare OPEB calculations.

**Key Control #2 (Manual - Valuation, Classification)** - OFM allocates each agency's liability by expenses reported in sub-object BD (Health, Life & Disability Insurance) to ensure OPEB balances are properly reported in the appropriate statement and opinion unit.

**Key Control #3 (Manual - Valuation, Classification, and Completeness)** - Kennessy Cavanah, OFM Statewide Accountant, prepares a year-end journal voucher to record the long-term liabilities balance using the actuary report and allocation schedule calculations. Another Statewide Accountant performs a detailed review over the OPEB excel workbook to ensure journal vouchers were supported by audited OPEB schedule amounts, accurately allocated to respective agencies and reporting funds, and accurately adjusted balances to ensure opinion units recorded state-wide balances and amounts in compliance with reporting requirements under GASB 75.

## Noted Weaknesses are as Follows:

**None.**

## I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows

*Procedure Step:* Key Control 1 (Manual)

*Prepared By:* BM2, 10/17/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To confirm the OFM Statewide Accountant reviews the results of the OPEB Schedule audit and census data testing to ensure the completeness and accuracy of the allocation percentages used to prepare OPEB calculations (key control 1 for Allocation of OPEB Amounts) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

# State of Washington

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control 1 (Completeness and Valuation):** The OFM Statewide Accountant reviews the results of the OPEB Schedule audit and census data testing to ensure the completeness and accuracy of the allocation percentages used to prepare OPEB calculations.

The understanding for this system is documented above in the "Controls - Allocation of OPEB Amounts" step.

### **1. Confirmation of Key Manual Control:**

We reviewed OFM's ACFR OPEB calculation workbook, "OPEB\_Worksheets\_2024", prepared by Kenney (Statewide Accountant), and noted the allocation amounts and supporting OSA/Milliman figures tied to our recalculation workbook from S1FinancialManagement-FS24. Kenney used SAO's audit to confirm allocation percentages for OPEB balances were complete and accurate. Within OFM's workbook, Kenney compared allocation percentages used in prior calculations to the current allocation percentages and made necessary changes to include new agencies/remove disbanded agencies and summarize Community and Technical college data for rollup in ACFR. We compared the updated allocation percentages to data in the OPEB audit (S1FinancialManagement-FS24) and confirmed OFM's source data for ACFR calculations agreed to the audited OPEB schedules.

We performed a review of the SAO Statewide OPEB Schedules Audit (S1FinancialManagement-FS24) to determine if OFM using the allocation data was reasonable. We reviewed underlying census data and actuary work of OSA and Milliman as part of S1FinancialManagement-FS24 and noted the following:

Census Data - FY24 is a roll forward year, therefore, census data and the underlying assumptions are not updated. We reviewed S1FinancialManagement-FS23 for results of census data testing, applicable to FY24 OPEB balances and noted the following: We reported 1 exit item in relation to census data testing as part of the audit. One agency had 9 employees that did not meet our expectations and were included in the census data when they shouldn't have or vice versa. The effect was isolated to the one agency and did not impact any OPEB balances.

Actuary Work - We reviewed the rely on work of specialist performed in S1FinancialManagement-FS24 over Milliman and OSA. We noted no exceptions and that we determined we could rely on the work of Milliman and OSA in relation to the OPEB schedules.

Based on substantive testing performed in S1FinancialManagement-FS23 and FS24, we determined the population used for ACFR reporting were

# State of Washington

complete and estimates were valued accurately. *No issues noted.*

## Noted Weaknesses are as follows:

None.

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows**

*Procedure Step:* Key Control 2 (Manual)

*Prepared By:* BM2, 10/24/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion.\*

### **Purpose:**

To confirm OFM allocates each agency's liability by expenses reported in sub-object BD (Health, Life & Disability Insurance) to ensure OPEB balances are properly reported in the appropriate statement and opinion unit (key control 2 for Allocation of OPEB Amounts) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls, however, we did note the following:

OFM's review of the OPEB allocation calculation was insufficient to ensure that the calculation was performed correctly. This resulted in various misstatements across opinion units. **See issue:** [V: OFM Allocation of OPEB Amounts (Part of ML)]. **See AOM:** [Aggregation of Misstatements (GAAP)].

## State of Washington

### Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**Key Control 2 (Valuation and Classification):** OFM allocates each agency's liability by expenses reported in sub-object BD (Health, Life & Disability Insurance) to ensure OPEB balances are properly reported in the appropriate statement and opinion unit.

The understanding for this system is documented above in the "Controls - Allocation of OPEB Amounts" step.

### **1. Confirmation of Key Manual Control:**

We obtained OFM's prepared allocation calculation workbook, "OPEB\_Worksheets\_2024\_.xlsx" from Kennesy Cavanah, Statewide Accountant. OFM uses BD expenses by rollup fund and posting agency to further allocate whole agency allocation percentages based on function and fund. The BD expense therefore helps to define the classification and allocation of OPEB benefits within each agency's overall allocation percentage. Rollup funds determine the appropriate opinion unit to report OPEB balances.

We noted all FYE 2024 expenses for subobject BD were exported and agency percentages were allocated across funds and statements by the amounts reported in sub-object BD. We confirmed OFM used all FYE 2024 BD expenses by running an independent query from the ACFR database. See [[OPEB Adjusted Allocation Recalculation](#)], tabs 'SAO ACFR Query BD\_FY24' for the documented SQL code and results. We noted SAO's total BD expenses for FYE 2023 (measurement date) was \$1,768,133,876.14. OFM included beginning balances in their exported data of BD expenses and totalled \$3,177,144,950.35.

We recalculated the adjusted allocation percentages based on agency head counts and expenses coded to sub-object 'BD', excluding beginning balances to remain consistent with calculations in previous years. See [[OPEB Adjusted Allocation Recalculation](#)], tab 'Mod Allocation % Comparison.' Our calculated allocation percentages varied from OFM's as a result of their calculation erroneously including beginning balances of the BD expense account. The differences in allocation percentage caused issues in the valuation of OPEB balances among opinion units and incorrect deferred inflows/outflows at a statewide level. See issue at [[V: OFM Allocation of OPEB Amounts \(Part of ML\)](#)].

### **Noted Weaknesses are as follows:**

OFM's review of the OPEB allocation calculation was insufficient to ensure that the calculation was performed correctly. **See issue in conclusion above.**



# State of Washington

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows**

*Procedure Step:* Key Control 3 (Manual)

*Prepared By:* BM2, 10/25/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion.:

#### **Purpose:**

To confirm OFM Statewide Accountant, prepares a year-end journal voucher to record the long-term liabilities balance using the actuary report and allocation schedule calculations (key control 3 for Allocation of OPEB Amounts) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls, however, we did note the following:

OFM's review of the OPEB allocation calculation was insufficient to ensure that the calculation was performed correctly. This resulted in various misstatements across opinion units. **See issue:** [V: OFM Allocation of OPEB Amounts (Part of ML)].

Testing Strategy.:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

**Key Control 3 (Valuation, Classification, and Completeness):** Kennesy Cavanah, OFM Statewide Accountant, prepares a year-end journal voucher to record the long-term liabilities balance using the actuary report and allocation schedule calculations. Another Statewide Accountant performs a detailed review over the OPEB excel workbook to ensure journal vouchers were supported by audited OPEB schedule amounts, accurately allocated to respective agencies and reporting funds, and accurately adjusted balances to ensure opinion units recorded state-wide balances and amounts in compliance with reporting requirements under GASB 75.

The understanding for this system is documented above in the "Controls - Allocation of OPEB Amounts" step.

## **1. Confirmation of Key Manual Control:**

We obtained OFM's JV to record OPEB balances as of June 30, 2024, JVOFM89. We reviewed OFM's JV workbook (JVOFM089\_OPEB\_DO\_DI\_Exp\_TOPEBL.xlsx) which included the JV, links to OFM's supporting calculation workbooks, and indication of review (emails from reviewer, notes and signature and date).

We reviewed OFM's allocation calculation workbook "OPEB\_Worksheets\_2024" that was used to determine OPEB balances by rollup fund. We agreed the JV to the supporting workbook's tab "JV Summary" with no exceptions.

We noted Kennesy Cavanah, Statewide Accountant, prepared the entry on 8/20/2024. Anna Quichocho, Financial Reporting Manager, reviewed and approved the entry on 8/23/2024. During our review of the calculation workbook (see key control 2), we identified errors in the calculation of allocation percentages. We noted this as a weakness.

## **Noted Weaknesses are as follows:**

OFM's review of the OPEB allocation calculation was insufficient to ensure that the calculation was performed correctly. **See issue in conclusion above.**

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

# State of Washington

## I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows

*Procedure Step:* Risk Assessment

*Prepared By:* BM2, 10/14/2024

*Reviewed By:* RKM, 10/23/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

#### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

#### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

## State of Washington

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

*Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

### **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

## State of Washington

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

# State of Washington

**Completeness - High**

**Valuation - High**

**Classification - High**

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

### **GASB Allocation of OPEB Amounts - Completeness, Valuation, Classification**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**Completeness - HIGH**

**Valuation - HIGH**

**Classification - HIGH**

## **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

To address the following risks:

**Completeness** - Members are inappropriately excluded from, or included in, the census data

**Valuation** - Census data does not reconcile to (agree with) the employer's payroll and personnel records or is not properly accumulated (maintained) for active and inactive members, causing errors in the computation of deferred outflows, total OPEB liability, and/or deferred inflows; The actuary uses incomplete (missing) or incorrect census data, causing errors in the computation of total deferred outflows, total OPEB liability, and/or deferred inflows; The actuary uses inappropriate assumptions or actuarial methods that are not in conformity with GASB Statement No. 75

**We will rely on the SAO audit S1FinancialManagement-FS24 for the accuracy of census data**

As part of S1FinancialManagement-FS24, we perform a review of census data to verify the head count figures representing active members in the OPEB plan are accurate, complete, and agree to agency records. We also verify that OFM's calculation of OPEB



## State of Washington

amounts are based on the same head count data used by HCA's actuaries. We will reference this work and ensure that head count figures used in OFM's OPEB balance calculations agree.

**We will rely on the SAO audit S1FinancialManagement-FS24 for the review of the actuarial valuation**

As part of S1FinancialManagement-FS24, we perform a review and rely on specialists, OSA (prepares the OPEB actuarial valuation) and Milliman (determines estimates related to OPEB, transactions subsequent to the measurement date). We will reference this work and ensure that figures used in OFM's OPEB balance calculations for ACFR agree.

To address the following risks:

**Valuation** - Deferred outflows of resources and deferred inflows of resources and OPEB expense are not properly calculated and reported in accordance with GASB Statement No. 75

**Classification** - There is a risk that the allocation between funds is not representative of the agencies included in that roll-up fund

**We will re-perform OFM's OPEB balance calculations to determine if deferred inflows, outflows, total OPEB liability, and all OPEB components are properly valued and classified in accordance with GASB 75/GAAP:**

- STEP 1: Review OPEB audit (S1FinancialManagement-FS24) to ensure we can rely on allocation percentages based on head counts. Obtain head count data to determine allocation percentages for ACFR purposes. Review and adjust head count data for cash basis agencies to ensure amounts were appropriately recorded for GAAP statements.
- STEP 2: Re-calculate adjusted allocation percentages based on sub-object BD (represents actual employer medical contribution expenditures). Obtain BD expenditures from ACFR database. Add rollup fund and reporting fields to the data to determine ACFR allocation percentages.
- STEP 3: Calculate OPEB Balances by Roll-Up Fund and Posting Agency. Allocate statewide OPEB balances from the actuarial valuation performed by OSA. Verify total from calculations agree to OSA actuarial valuation.
- STEP 4: Tie out recalculated OPEB balances by roll-up fund and agency to AFRS data. Verify the financial statement balances agree to AFRS data and SAO's recalculation work.

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### I.5.PR.G - OPEB - Liability (Current & Noncurrent), Deferred Inflows, Deferred Outflows

<i>Procedure Step:</i>	Substantive Test
<i>Prepared By:</i>	BM2, 10/22/2024
<i>Reviewed By:</i>	RKM, 11/18/2024

# State of Washington

## Purpose/Conclusion:

### **Purpose:**

To determine the following:

- whether all non-current liabilities as of the end of the period were reported.
- whether non-current liabilities were reported at properly valued or calculated amounts.
- whether financial statements properly classify non-current liabilities in conformity with generally accepted accounting principles (GAAP).

### **Conclusion:**

We determined the following:

- all non-current liabilities as of the end of the period were reported.
- non-current liabilities were **not** reported at properly valued or calculated amounts. See issue at [V: OFM Allocation of OPEB Amounts (Part of ML)].
- financial statements properly classify non-current liabilities in conformity with generally accepted accounting principles (GAAP).

## Testing Strategy:

### **Completeness**

The following is a list of **considerations** for testing the completeness assertion for non-current liabilities. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Long-Term Debt**

Review minutes or legislative proceedings and enactments, and inquire whether all debt bearing the name of the reporting entity or any of its component entities is identified and is properly disclosed in the financial statements and notes.

Confirm publicly-issued bonds by searching EMMA and/or the Washington State Department of Commerce sites.

*State agencies and local governments are required to report all bond issuances (including anticipation notes and privately placed debt) to Dept of Commerce per RCW 39.44.210. Bond underwriters and dealers are required by the SEC per 17 CFR 240.15c2-12 to report information on bond issuances to EMMA. Issuers are further required to post continuing disclosure requirements to EMMA. Dept of Commerce's Bond Clearinghouse can be accessed at: <https://fortress.wa.gov/com/buc/BondFormSearch.aspx> EMMA can be accessed at: <http://emma.msrb.org/Default.aspx>. NOTE: these sources may not be complete if issuers have not done required reporting.*

Confirm amounts outstanding with lenders or fiscal agents using blind confirmations. *Note: this test also evidences existence.*

Scan check register for vendors that may represent a lending institution or lessee and determine if payments made were for long term debt or capital leases.

# State of Washington

Review documentation for operating leases to determine if these should have been accrued as capital leases. *Note: this test also addresses the valuation assertion.*

Review contracts or inquire as to the existence of any guarantees or commitments related to the issuance of debt of other organizations.

Verify debt balances to source amortization schedules from authorizing resolutions or ordinances, agreements or issuance documents and verify all early retirements. *Note: this test only provides evidence about completeness of previously reported debt.*

**Net OPEB Obligations (for entities that have implemented GASB 45)** - Auditors should use the OPEB Audit Plan workpaper available in the Store for auditing OPEB liabilities.

**Pollution Remediation Obligations (for entities that have implemented GASB 49)** - Auditors should use the Pollution Liability Audit Plan workpaper available in the Store for auditing pollution remediation liabilities.

## **Classification**

The following is a list of **considerations** for testing the classification assertion for non-current liabilities. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Review source documents to verify that non-current liabilities are obligations of the reporting fund, rather than some other fund.

Review journal entries that re-classify non-current debt.

To verify whether general obligation debt should be reported (in whole or in part) as a liability of a proprietary fund, review documentation and transactions for support of the intent and ability to pay general obligation debt from proprietary funds.

Trace amounts due in within one year per debt-repayment schedules to check that it was properly shown as a current liability. Note that lines of credit and demand debt (debt that is payable at any time upon demand of the holder) should be classified as a current liability.

## **Valuation**

The following is a list of considerations for testing the valuation assertion for non-current liabilities. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Recalculate or review entity calculation of capital lease liabilities

Recalculate or review entity calculation of estimated long-term liabilities

Recalculate or review entity calculation of imputed interest on non-interest-bearing notes or other liabilities.

Recalculate or review entity calculation of accrued termination benefits (see GASB 47 for requirements)

Recalculate or review entity calculation of compensated absences liability (see GASB 16 for requirements). If reviewing the entity's calculation, compare the formulas used against the entity's policy; for instance, if an auditee pays 25% for accumulated sick leave

## State of Washington

upon retirement but not if the employee leaves for other reasons, we would expect the formula to incorporate projections of the proportion of employees continue employment until retirement.

Recalculate or review entity calculation of landfill closure and post-closure costs (see GASB 18 for requirements). If reviewing the entity's calculation, evaluate the formula for reasonableness; for instance, cost elements should include facilities and equipment, capping and post-closure monitoring. Verify there is an annual reevaluation of the costs by reviewing their documents supporting that the yearly cost estimate has been updated.

**Net OPEB Obligations (for entities that have implemented GASB 75)** - Auditors should use the GASB 75 OPEB Balances Baseline Testing and the corresponding GASB 75 Testing Strategy workpaper available in the Store for auditing OPEB liabilities.

**Pollution Remediation Obligations (for entities that have implemented GASB 49)** - Auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation liabilities.

Guidance/Criteria.:

**Add the Guidance/Criteria for each relevant assertion from the TeamStore. You may also include other resources that you used for testing.**

Record of Work Done.:

**Substantive tests performed to meet the Completeness assertion:**

**Identified Risk(s):** Members are inappropriately excluded from, or included in, the census data

We will rely on the SAO audit S1FinancialManagement-FS24 for the accuracy of census data. As part of S1FinancialManagement-FS24 we:  
performed a review of census data to verify the head count figures representing active members in the OPEB plan are accurate, complete, and agree to agency records  
verified that OFM's calculation of OPEB amounts are based on the same head count data used by HCA's actuaries

We will reference this work and ensure that head count figures used in OFM's OPEB balance calculations agree. Based on our review of testing procedures and results of the OPEB schedule audit, we determined we could place reliance on the procedures performed as part of SAO audit S1FinancialManagement-FS24. We determined the quality and quantity of evidence obtained was sufficient and appropriate to address ACFR risks.

**Testing Results**

We relied on SAO's audit S1FinancialManagement-FS24 for testing the completeness of head count related census data (for allocation purposes and data used by actuaries). We reviewed the following to address completeness risks:

# State of Washington

## Completeness of Census Data

We reviewed the S1FinancialManagement-FS24 issues and noted none impacted the completeness of census data. We determined the census data was complete and members were appropriately included in the census data.

## Completeness of Data Used in the Calculation of OPEB Balances

We reviewed procedures related to the work of specialists (OSA and Milliman, located in C.2). No exceptions were noted. We determined we could rely on the work performed by OSA and Milliman.

*No issues noted.*

## **Substantive tests performed to meet the Valuation assertion:**

**Identified Risk(s):** Census data does not reconcile to (agree with) the employer's payroll and personnel records, or is not properly accumulated for active and inactive members, causing errors in the computation of deferred outflows, total OPEB liability, and/or deferred inflows; The actuary uses incomplete (missing) or incorrect census data, causing errors in the computation of total deferred outflows, total OPEB liability, and/or deferred inflows; The actuary uses inappropriate assumptions or actuarial methods that are not in conformity with GASB Statement No. 75

We relied on the SAO audit S1FinancialManagement-FS24 for the accuracy of census data and actuarial valuation. As part of S1FinancialManagement-FS24 we:

- performed a review of census data to verify the head count figures representing active members in the OPEB plan are accurate, complete, and agree to agency records
- verified that OFM's calculation of OPEB amounts are based on the same head count data used by HCA's actuaries
- performed a review and relied on specialists, OSA (prepares the OPEB actuarial valuation) and Milliman (determines estimates related to OPEB, transactions subsequent to the measurement date).

## Testing Results

We reviewed OFM's OPEB balance calculations for ACFR, from "OPEB\_Worksheets\_2024\_.xlsx", to agree headcount and allocation percentages to audited schedules. Allocation percentages used in reporting ACFR related OPEB balances tied to S1FinancialManagement-FS24 without exception. Based on our review of testing procedures and results of the OPEB schedule audit, we determined we could place reliance on the procedures performed as part of SAO audit S1FinancialManagement-FS24. We determined the quality and quantity of evidence obtained was sufficient and appropriate to address ACFR risks. The allocation percentages used in ACFR reporting were based on complete and accurate census data (See C.1.2 in S1FinancialManagement-FS24) and actuary's assumption were appropriate based on our review of specialists, in conformity with GASB 75 (See C.2 in S1FinancialManagement-FS24).

*No issues noted.*

**Identified Risk(s):** Deferred outflows of resources and deferred inflows of resources and OPEB expense are not properly calculated and

# State of Washington

reported in accordance with GASB Statement No. 75

We re-performed OFM's OPEB balance calculations to determine if deferred inflows, outflows, total OPEB liability, and all OPEB components are properly valued and classified in accordance with GASB 75/GAAP.

## Testing Results

STEP 1: Review OPEB audit (S1FinancialManagement-FS24) to ensure we can rely on allocation percentages based on head counts. Obtain head count data to determine allocation percentages for ACFR purposes. Review and adjust head count data for cash basis agencies to ensure amounts were appropriately recorded for GAAP statements.

See details of review above. We confirmed allocation percentages used in ACFR reporting agree to the audited OPEB schedules. For measurement date (6/30/2023) this included 134,978 active and eligible employees. *No issues noted.*

STEP 2: Re-calculate adjusted allocation percentages based on sub-object BD (represents actual employer medical contribution expenditures). Obtain BD expenditures from ACFR database. Add rollup fund and reporting fields to the data to determine ACFR allocation percentages.

See [\[OPEB Adjusted Allocation Recalculation\]](#). We performed the following:

Obtained the FYE 06/30/2024 BD expenses from the ACFR database. See tab 'SAO ACFR Query BD\_FY24.'

We added reporting fields to the BD data through power query. We used OFM's tables that summarized financial statement reporting fields. We tied the tables to SAAM Chapter 75 to ensure the accuracy of the financial statement mapping. See [\[OPEB Power Query Process\]](#) for the steps we took to assign the appropriate reporting fields. See tab 'BD with Reporting Fields FY24.' for the results.

We summarized the BD expense report by agency, roll-up fund, and posting agency. See tab '23 BD Allocation %.' We used conditional formatting to identify agencies that reported in multiple funds. We manually calculated the percent of BD expenses reported by roll-up fund and posting agency for each agency. We ensured the accuracy of the BD reporting percentages tied to the number of listed agencies used for head-count allocations. We noted all agencies (state agencies and component units) were included. We identified the following component units that would have to be removed for ACFR reporting: 106 Washington Economic Development Finance Authority - FMZ 700A, 148 Washington State Housing Finance Commission - FMZ 700A, 599 Washington Health Care Facilities Authority - FMZ 700D

We used a power query to match the agency number as reported on our BD expense data to the allocation percent reported in the audited WA state-wide OPEB report (S1FinancialManagement-FS24, Schedule 1). We multiplied the BD allocation by the agency allocation to determine the adjusted allocation percentage. See tab 'Modified Allocation %.'

We summarized the adjusted allocation percentage by roll-up fund and posting agency and compared our calculation of the adjusted allocation percentages with OFM's adjusted allocation percentages. **We noted several differences between OFM's calculation and SAO's calculated adjusted percentages. OFM included the beginning balance of expenses coded to subobject BD in their calculation of allocations. This error caused variances in allocation percentages by rollup fund. OFM's modified allocated percentages used for reporting OPEB to ACFR are incorrect. This resulted in small percentage differences by opinion unit, which**

## State of Washington

caused reported amounts to differ. See tab 'Mod Allocation % Comparison.' See issue at [\[V: OFM Allocation of OPEB Amounts \(Part of ML\)\]](#). We determined the misstatement effect as part of step 4 below.

STEP 3: Calculate OPEB Balances by Roll-Up Fund and Posting Agency. Allocate statewide OPEB balances from the actuarial valuation performed by OSA. Verify total from calculations agree to OSA actuarial valuation.

See [\[OPEB Balances by Adjusted Allocation and Rollup Fund\]](#). We performed the following:

We used our recalculation of the modified allocation percentages from the Adjusted Allocation recalculation workbook [\[OPEB Adjusted Allocation Recalculation\]](#) to recalculate total OPEB balances. We carried forward the "Mod Allocation % Comparison" tab (calculated above) and the 2016-2023 head counts from the State of Washington's OPEB Schedules to use in our workbook.

We aggregated adjusted percentage allocations for fiscal years 2016-2023 in tab 'Modified Allocation % Fund&Func' and inquired about any changes or new reporting in rollup fund/posting agencies with Kennesy Cavanah, OFM Statewide Accountant.

Next, we calculated change in agency proportionate share deferred outflows and inflows for FY24. See tab 'FY 2024 DO-DI Determination.' For determining allocation of OPEB balances within a government, GASB 75 prescribed OPEB allocation methodologies must be consistent with pension allocations. We calculated the change in agency proportionate share based on the methodology used for pensions as prescribed by GASB 68, 74, and 85. We used audited OPEB amounts from S1FinancialManagement-FS24 and OSA report amounts to allocate based on the adjusted allocation % for rollup fund/posting agency.

Once change in agency proportionate share was determined, we calculated amortization schedules and balance of deferred outflows and inflows as of 06/30/2024. We noted OFM and our calculations used a nine year amortization period which was the actuarial determined average expected remaining service life of all active and inactive members (as prescribed by GASB 75). See tab 'DO-DI Amort Sched.'

We calculated all reported OPEB balances (including all elements of deferred outflows and inflows) by roll-up fund and posting agency. See tab 'OPEB Balances by Rollup Fund.' Note, we calculated the OPEB liability by short-term and long-term amounts. Short-term OPEB liabilities totaled the transactions subsequent to the measurement date. Long term OPEB liabilities were calculated as total OPEB liability less the short term liability.

STEP 4: Tie out recalculated OPEB balances by roll-up fund and agency to AFRS data. Verify the financial statement balances agree to AFRS data and SAO's recalculation work.

See [\[AFRS Tie Out to OPEB Recalculation\]](#). We performed the following:

We used our calculation of OPEB balances by roll-up fund and posting agency from the steps above, tab 'OPEB Balances by Rollup Fund.' We aggregated OPEB balances by roll-up fund using a pivot table in tab 'Pivot - Balances by Rollup Fund.' We identified the amounts allocated for cash basis component units that would need to be adjusted since they are not included in AFRS (worksheet adjustments). Those amounts are posted in rollup fund FMZ for the following agencies:

106 - Washington Economic Development Finance Authority

148 - Washington State Housing Finance Commission

## State of Washington

599 - Washington Health Care Facilities Authority

We ran a query for all OPEB balances in the ACFR database. See tab 'AFRS GL Query 2024.' We compared OPEB amounts by roll-up fund in tab 'AFRS Balance to OPEB Sched.' We tied out balances by general ledger accounts to ensure our calculations by roll-up fund were correct. We also tied out significant balances as documented in the leadsheet to ensure our re-calculation tied to the reported balances. We identified variances due to OFM using incorrect allocation percentages by rollup fund for ACFR reporting. This resulted in variances at the opinion unit level for all balances identified in the leadsheet. We determined 6 balances across opinion units were misstated by amounts above their applicable floor. See issue at [V: OFM Allocation of OPEB Amounts (Part of ML)]. This included the following:

Statement of Net Position (Government Wide) - Business-Type Activities:

Long Term Liabilities Due in More Than One Year (Other Post Employment Benefits Obligations) was overstated by \$7.05 million

Deferred Inflows of Resources (OPEB) was understated by \$8.63 million

Statement of Net Position (Proprietary Funds) - Health Insurance:

Other Long Term Liabilities - Noncurrent (Other Post Employment Benefits) was overstated by \$155 thousand.

Statement of Net Position (Proprietary Funds) - Higher Education Student Services:

Other Long Term Liabilities - Noncurrent (Other Post Employment Benefits) was overstated by \$8.75 million

Deferred Outflows of Resources (OPEB) was overstated by \$946 thousand

Deferred Inflows of Resources (OPEB) was understated by \$7.00 million

### **Substantive tests performed to meet the Classification assertion:**

**Identified Risk(s):** There is a risk that the allocation between funds is not representative of the agencies included in that roll-up fund

We re-performed OFM's OPEB balance calculations to determine if deferred inflows, outflows, total OPEB liability, and all OPEB components are properly valued and classified in accordance with GASB 75/GAAP.

### **Testing Results**

See testing results above for steps performed (steps 1 through 4). Amounts appeared to be reported properly as short and long term (in conformity with GAAP), however, our testing identified variances in reporting at the opinion unit level as a result of inaccurate allocations for rollup funds. We identified 6 balances across opinion units that were misstated. OPEB balances were not representative of the rollup funds and agencies included. See issue at [V: OFM Allocation of OPEB Amounts (Part of ML)].

### **I.6.PRG - Long & Short Term Liabilities: Bonds**

*Procedure Step:* Summary & Conclusion



# State of Washington

*Prepared By:* JAG, 10/1/2024  
*Reviewed By:* RKM, 11/23/2024

## Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

## Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

## State of Washington

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing

## SAO Audit Policy [3210](#) – Audit Evidence

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We determined the results of substantive tests do not indicate a need to modify our risk assessment (IR, CR and RMM).

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We determined the quality and quantity of evidence obtained was sufficient and appropriate.

### **I.6.PRG - Long & Short Term Liabilities: Bonds**

*Procedure Step:* Understanding of Line Item

*Prepared By:* JAG, 5/3/2024

*Reviewed By:* RKM, 6/18/2024

Purpose/Conclusion:

### **Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

# State of Washington

## **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

## **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associated with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

## **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large*

## State of Washington

*percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria:

Record of Work Done:

### **(1) Prior Audit Exceptions:**

We did not identify any prior audit exceptions.

### **(2) Composition & Change Analysis:**

Line Item Lead Sheet: [\[Line Item Lead Sheet\]](#)

### **Governmental Activities - Long Term Liabilities Due Within One Year (Bonds)**

### **Governmental Activities - Long Term Liabilities Due in More Than One Year (Bonds)**

The Office of the State Treasurer (TRE) manages the state's debt as one of their core functions. The State issues debt via bond sales to finance some of the state's major capital and transportation projects and issues certificates of participation (COPs) to finance real estate and equipment for state agencies and local governments.

### **Composition of the Line Item and Planned Audit Coverage:**

The following GL account balances roll up into the line item: \*Note: GL Codes listed in [SAAM 75.40.20](#)

Long-term Liabilities Due Within One Year (Bonds):

**GL 5161 - General Obligation (GO) Bonds Payable**

**GL 5162 - Revenue Bonds Payable**

**GL 5164 - Zero-Coupon (GO) Rate Bonds Payable**

**GL 5169 - Other Bonds Payable**

The bolded GL accounts (GLs 5161, 5162, 5164, 5169) have been selected for audit, providing 100% coverage of the line item.

## State of Washington

Long-term Liabilities Due in More than One Year (Bonds):

GL 5212 - Accreted Interest Payable

**GL 5261 - General Obligation Bonds Payable**

**GL 5262 - Revenue Bonds Payable**

GL 5264 - Zero-Coupon GO Bonds Payable

GL 5269 - Other Bonds Payable

GL 5273 - COP Notes Payable

GL 5297 - Fees Payable

GL 5299 - Other Obligations

The bolded GL accounts (GLs 5261, 5262) have been selected for audit, providing 98.14% coverage of the line item. TRE shows a balance in GLs 5212, 5264, and 5297, but their inclusion does not significantly change the audit coverage, so it is omitted to prevent over-auditing.

### **(3) Updates to Significant Account Matrix:**

No changes required.

### **I.6.PRQ - Long & Short Term Liabilities: Bonds**

*Procedure Step:* Controls - TM\$

*Prepared By:* JAG, 4/29/2024

*Reviewed By:* RKM, 8/12/2024

Purpose/Conclusion:

#### **Purpose:**

To gain an understanding of internal controls.

#### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

**The following procedures are required for all material systems:**

## State of Washington

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control

## State of Washington

When (or how often) is the control applied

Who performs the control

As needed, the experience, knowledge and attitude of the person applying the control

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any exceptions or alternative processing to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**



# State of Washington

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

### [Financial Statement Audits](#) Planning Guide

Record of Work Done:

Internal controls in the Treasury Management System (TM\$) address the following balance(s):

**Governmental Activities - Long Term Liabilities Due Within One Year (Bonds)**

**Governmental Activities - Long Term Liabilities Due in More Than One Year (Bonds)**

For the following assertions:

**Completeness:** That all bonds payable amounts occurring during the period are not identified and recorded.

**Valuation:** Since bond payable balances are constantly changing due to new issuances and payment of principal and interest, there is a risk that bonds payable amounts are reported at incorrect amounts.

**Classification:** Amortization schedules calculating short and long term portions could be misstated or not updated resulting in bonds that are incorrectly classified between short and long term.

**Auditor's Note:** The ROWD references long-term liabilities due within one year and long-term liabilities due in more than one year. "Long-term liabilities due within one year" describes the balance on the State's financial statements representing the current portion of issued bonds and should not be labeled as a short-term liability. OFM does not use GL 5121 (Matured Bonds Payable) to record bond balances issued by TRE maturing in less than 1 year. SAAM lists all "GL 516X" accounts as "Short-term Bonds Payable," which includes GL accounts 5161, 5162, 5164, and 5169. When discussing the current portions of long-term liabilities with TRE staff, use the term "short-term bonds payable" to describe the current portion to avoid confusion.

### **Gain an Understanding of Internal Controls**

To update our understanding of internal controls, we conducted a Teams meeting on 4/25/24 with: Leslie Yonkers, Debt Financial Officer and Austin Goble, Bond Program Manager. TRE referred us to their "Debt and Credit Analysis" covering high level information regarding bonds here: [\[2024 Debt and Credit Analysis - For The Web - Final.pdf \(wa.gov\)\]](#). The report includes additional details about the types of bonds issued, credit ratings, other obligations, and borrowing costs. Unless otherwise noted, TRE uses the Treasury Management System (TM\$) as their accounting system over the line items.

### **Debt Issuance Processes:**

#### **Phase 1A - Bond Sale Process**

# State of Washington

## Non-COP (Certificate of Participation) Bonds:

TRE's debt management staff track the Legislative Session to determine which programs will require new debt issuance. Once the Session is over, Austin Goble, Bond Program Manager, prepares all the details to be input into TM\$ and Leslie Yonkers, Debt Financial Officer, along with Austin reviews bond details for accuracy. Austin then looks at the cash flow estimate for fund 057 (State Building Construction Account). The cash flow estimate reconciles new appropriations with agency funds appropriated and spent from fund 057 for maintenance and construction projects. For the three agencies that have individual authority to spend from a specific bond authorization (Department of Transportation, Department of Ecology, and Department of Commerce), Leslie asks the agencies to estimate their cash flow needs for the next six months. In addition, the Secretary of the Department of Transportation sends a letter requesting bond proceeds for its financial needs before a bond sale.

## COP Bonds:

State agencies and municipalities enter into COPs and because they do not benefit the state as a whole, they do not count towards the state's debt limit. COP bonds do not require legislative approval unless it is for constructing a building or a large service based project. COP bonds typically have a shorter maturity date. The financed project or leases determine the COP bond amount, which the bond staff enter into TM\$. COP bond sales follow the same process as other bond sales (described below) with exception to the approval process (described above).

## All Bonds:

The State sold the following bonds in fiscal year 2024:

- July 25 General Obligation Bonds (Taxable), 2024T
- July 25 MVFT/VRF General Obligation Bonds, 2024B
- July 25 Various Purpose General Obligations Bonds, 2024A
- October 26 Certificates of Participation, Series 2023C
- November 7 MVFT/VRF General Obligations Refunding Bonds, R-2024B
- November 7 Various Purpose General Obligation Refunding Bonds, R-2024A
- January 23 MVFT/VRF General Obligation Bonds, 2024D
- January 23 Various Purpose General Obligation Bonds, 2024C
- February 26 Certificates of Participation, 2024A
- March 26 MVFT/VRF General Obligation Refunding Bonds, R-2024C
- June 25 Certificates of Participation, 2024B
- June 25 Various Purpose General Obligation Refunding Bonds, R-2025A
- June 25 General Obligation Bonds (Taxable), 2025T
- June 25 MVFT/VRF General Obligation Bonds, 2025B
- June 25 Various Purpose General Obligation Bonds, 2025A

Austin works with the state's municipal advisors to determine a good time for bonds to enter the market. The State typically issues new money bonds on a semiannual basis. For 'advance' refundings, policy sets the savings threshold to a present value savings of at least five percent of the

## State of Washington

principal amount of the refunding debt issued. A 'current' refunding transaction requires a graduated present value savings depending on the years between call and final redemption, which varies between 1% and 5%. The State Finance Committee may, and regularly, grants the Treasurer the authority to enter the market without pre-approval for new money and refunding bond issuance, through a resolution, as provided by a 2010 amendment to [RCW 39.42](#). Public Law 115-97 eliminated the federal tax exemption for interest income earned on advance refunding bonds for any municipal bond issued after tax year 2017.

When a bond is ready to be issued, Leslie Yonkers inputs the agency request for bond proceeds into TM\$. Austin Goble reviews and adjusts as necessary prior to sending it to state's the bond counsel. Austin will compile the chapters, laws and TM\$ authorization numbers and forwards to the bond counsel to double check that the requests are within the bond authority. The bond counsel drafts a resolution for the State Finance Committee, who reviews applicable laws and regulations, IRS rules, and other legal aspects of the bond issuance for the state. At the same time, the municipal advisors or TRE, in cooperation with the municipal advisors, prepare all the preliminary numbers, such as level of debt service. Typically, TRE prepares preliminary work and the municipal advisors review. For refundings, the municipal advisors prepare preliminary work and TRE reviews.

### **Phase 1B - Preparation for Bond Issuance**

When the bond counsel finishes writing the resolution and the municipal advisors and TRE finalize the preliminary numbers, Austin reviews the resolution to ensure they followed all applicable rules and regulations. Austin uses DBC Finance, an external municipal finance sizing and structuring software, to recalculate the numbers and see if they agree with the municipal advisors' amounts.

The state's Disclosure Council prepares the "Preliminary Official Statement" (POS) in conjunction with the Deputy Treasurer, Jason Richter, Debt Management division. TRE requests input regarding the correctness and completeness of the document from various state agencies, who then certify their review in writing. Dawn Leopardo, Debt Program Analyst, prepares and Austin Goble confirms the debt summary tables for Appendix A. TRE's Assistant Attorney General, Municipal Advisors, Bond Counsel, Disclosure Counsel, Deputy Treasurer, Debt Management division, Austin, and Leslie each receive a copy of this POS to review for format and substance. When approved, Whitney Trumbly, Compliance Officer, ensures the POS is posted on TRE's website and was sent electronically to ImageMaster's MuniOS distribution platform. The POS serves as the prospectus for underwriters and investors.

#### Negotiated Bond Sales (infrequent, specialized sale)

Negotiated bond issues occur when a bond is specialized or has a unique feature that appeals to a very limited market (e.g. when triple pledge bonds are issued with which the general investing public is not familiar). For a bond sale using the negotiated method, instead of receiving bids from underwriters, TRE posts a request for qualifications and request for proposals to hire underwriters who will underwrite the bonds, creating a pool of candidates. TRE conducts most bond sales on a competitive basis unless there are unique circumstances that would require the sale to be executed via the negotiated sale method.

#### Competitive Bond Sales (more frequent) – Winner is Lowest True Interest Cost (TIC)

All bidders for a competitive sale are pre-registered with i-Deal Prospectus (and its sale platform, "Ipreo"). On the day of the competitive bond sale, Ipreo invites underwriters to submit bids. TRE announces the winner based on who has the lowest TIC. All of the bids and the TIC % are posted on TRE's website at: [\[Bond and COP Sale Results | Office of the Washington State Treasurer\]](#).

TRE holds bond sales semi-annually. The State Finance Committee approval of the sales are open to the public. If there are multiple series or bid

## State of Washington

groups, each bid series is scheduled 15 to 30 minutes apart from each other. Austin shares the incoming bids via Teams or Zoom for everyone to observe. Debt Management members, Bond Counsel, and Municipal Advisors attend the sale virtually. Ipreo displays the Bidder Name and the TIC computed by the system from lowest to highest. TRE staff and municipal advisors verify the TIC to ensure it is correct prior to awarding the apparent winning bidder (the one with the lowest TIC). Once staff and advisors confirm the calculations and compliance with bid parameters, TRE selects and notifies the bidder with the lowest cost. A 90 minute deadline for wiring the good faith deposit starts following notification sent to the underwriter via Ipreo. Leslie receives the winning bidder's contact information from the municipal advisor and emails them information for wiring the good faith deposit. Leslie periodically logs into the bank account to see if winners wired the deposit. Austin and the other municipal advisors can resize or adjust bonds to meet proceeds requirements and desired debt structure (e.g. level debt service).

Leslie prepares the A8 form to record the good faith deposit and Stephanie Richardson, COP Financial Analyst, reviews it. Once reviewed, the Deputy Treasurer of Debt Management, Bond Program Manager (Austin), and Disclosure Counsel prepare the bond sale "Final Official Statement." Whitney ensures it is printed and posted on TRE's website while the bond disclosure counsel sends an electronic copy to ImageMaster. The municipal advisors send the closing letter to the underwriter. TRE also posts final bond sale information to the [EMMA website](#), which is an additional measure of transparency above TRE's required level of public disclosure.

Leslie then prepares a spreadsheet to determine the allocation of the bond proceeds, the underwriter's discount, and the issuance costs to the different agencies/funds. Austin reviews the spreadsheet for accuracy and that it matches the municipal advisors' numbers and the closing memo. Leslie also uses the spreadsheet to track and reconcile prepared A8 forms and allocates the bond proceeds to the correct funds.

### **Phase 2 - Receipt of Bond Sale Proceeds**

The bond purchasers (underwriters) transfer bond proceeds, less the underwriter's discount, to TRE about two weeks after the sale. The wire must match the closing memo. Leslie prepares the A8 form in TM\$ to record the receipt of bond proceeds and allocate the net proceeds to the appropriate funds. TM\$ uploads these transactions to AFRS automatically. Leslie runs the Enterprise report afterward to ensure that cash was properly posted to the recipient funds on a monthly basis in TM\$ (**Key Control 1 - Valuation, Completeness, and Classification**). Dawn prepares tables for TM\$ based on final numbers provided by the municipal advisors. Austin reviews the tables for accuracy, uploads the data to the TM\$ database, and creates new bond payment amortization schedules. Dawn then verifies the data imported into TM\$ by Austin for accuracy and completeness against all originally prepared forms (**Key Control 2 - Valuation, Completeness, and Classification**).

### **Phase 3 - Bond Debt Service Payment**

US Bank, the Fiscal Agent, posts monthly payments due for the following month on its website. This amount includes interest and principal for all bonds issued. Leslie downloads this invoice (CSV file) to prepare for payment. The invoice details the scheduled payment for State of Washington Bonds, including refunded bonds being paid by an escrow bank. US Bank publishes the invoice approximately 15 days prior to the due date of the payments.

Leslie imports the CSV file from US Bank into TM\$ and runs a "TRE to US Bank" reconciliation report. She pays the amount stated on US Bank's invoice unless the reconciliation identifies significant variances between the two sources. Typically the reconciliation shows a difference of only a few cents (**Key Control 3 - Completeness and Valuation**). To fix significant variances, Leslie emails her contact at US Bank to reconcile with the bank. Austin would work with Leslie to ensure the fix correctly remedies the issue.

## State of Washington

Leslie forces TM\$ to automatically prepare four main types of JVs:

- JV for an ACH wire that pays US Bank from various debt service funds on the payment date.

- JV to transfer same day debt service through the general fund (done for: DES, OOSPI, UW, WSU, and DOT).

- JV to reimburse the general fund from agencies required to do so (see above bullet).

- JV for payments made on principle in addition to interest payments, which reduces the principle outstanding in fund 999 - general long term debt account.

Stephanie Richardson, COP Financial Analyst, reviews and approves the JVs and reviews the payment, and the Assistant or Deputy Treasurer approves the debt service payment. The Cash Management division receives approved forms and sets up a 2 day ACH file to send out the money. TRE maintains all of these transfer documents in PDF. TRE saves these PDFs for their full retention length (33 years).

### **How transactions are recorded in AFRS:**

Leslie prepares all of the monthly transactions in TM\$ (refunding, debt service payments, etc.) that are related to the calculation of the current bond payments which effects the long-term liabilities (due within one year) and long-term liabilities (due in more than one year). She prepares the batches in TM\$ for the reconciliation to AFRS and Stephanie reviews and approves them. This reconciliation to AFRS ensures that the amount in AFRS the long-term liabilities (due within one year) and long-term liabilities (due in more than one year) matches the amortization schedules in TM\$ for all bond issues. Once approved, TM\$ releases the batch and operations uploads them into AFRS as a part of end-of-day processing. Leslie receives the "In Process Report" (exception report) on the following day which she uses to ensure that all transactions posted properly in AFRS (**Key Control 4 - Completeness and Classification**). The exception report runs every morning and only provides exceptions if an error occurs. The exception report most commonly identifies miscoded items. Leslie and Stephanie, as needed, updates information in AFRS to resolve any exceptions.

### **Key controls are as follows:**

**Key Control 1** - The Debt Financial Officer prepares the A8 form in TM\$ to record the receipt of bond proceeds and allocate the net proceeds to the appropriate funds. TM\$ uploads these transactions to AFRS automatically at the end of the day. The Officer runs the Enterprise report afterward to ensure that cash was properly posted to the recipient funds monthly in TM\$ (**Valuation, Completeness, Classification**).

**Key Control 2** - The Debt Program Analyst prepares tables for TM\$ based on the final numbers report package prepared by the state's municipal advisors. The Bond Program Manager reviews the tables for accuracy, and updates TM\$, which creates new bond payment amortization schedules. The Analyst then verifies the data imported into TM\$ by the Program Manager for accuracy and completeness against all originally prepared forms (**Valuation, Completeness, and Classification**).

**Key Control 3** - To process monthly bond service payments, the Debt Financial Officer imports the CSV file from US Bank into TM\$ and runs a "TRE to US Bank" reconciliation report. The Officer pays the amount stated on US Bank's invoice unless the reconciliation identifies significant variances between the two sources. Typically the reconciliation shows a difference of only a few cents (**Completeness and Valuation**).

**Key Control 4** - The Debt Financial Officer prepares all of the monthly transactions in TM\$ (refunding, debt service payments, etc.) that are related to the calculation of the current bond payments which effects the the long-term liabilities (due within one year) and long-term liabilities (due in more than one year). The Officer prepares the batches in TM\$ for the reconciliation to AFRS and the COP Financial

## State of Washington

Analyst reviews and approves them. This reconciliation to AFRS ensures that the amount in AFRS the long-term liabilities (due within one year) and long-term liabilities (due in more than one year ) matches the amortization schedules in TM\$ for all bond issues. Once approved, TM\$ releases the batch and operations uploads them into AFRS as a part of end-of-day processing. The Officer receives the "In Process Report" (exception report) on the following day which she uses to ensure that all transactions posted properly in AFRS. The exception report runs every morning and only provides exceptions if an error occurs **(Completeness and Classification)**.

### Noted Weaknesses are as Follows:

None.

### I.6.PRG - Long & Short Term Liabilities: Bonds

*Procedure Step:* Key Control #1 - TM\$ (Manual)

*Prepared By:* JAG, 4/29/2024

*Reviewed By:* RKM, 6/18/2024

Purpose/Conclusion.

#### **Purpose:**

To confirm the process to record a bond sale and its associated receipt of funds (key control #1 for TM\$) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy.

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

## State of Washington

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood*

## State of Washington

*of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done.:



# State of Washington

## **Key Control 1 - (Valuation, Completeness, Classification)**

The Debt Financial Officer prepares the A8 form in TM\$ to record the receipt of bond proceeds and allocate the net proceeds to the appropriate funds. TM\$ uploads these transactions to AFRS automatically at the end of the day. The Officer runs the Enterprise report afterward to ensure that cash was properly posted to the recipient funds monthly in TM\$.

The understanding for this system is documented above in the "Controls - TM\$" step.

### **1. Confirmation of Key Manual Control:**

We reviewed a Cash Receipt (A8) for \$739,727,782.45 for VP GO Bonds (Taxable) Series 2024C, sold January 23, 2024. Leslie Yonkers, Debt Financial Officer, prepared and signed the A8 on 1/26/2024, Stephanie Richardson, COP Financial Analyst, approved/signed it on 1/30/2024, and validated in a batch process on 2/7/2024.

We reviewed the allocation spreadsheet "2024CD Allocation" prepared by Leslie Yonkers, Debt Financial Officer, for the 2024C bond proceeds accounting allocations and supporting information. **No issues Noted.**

We reviewed an AFRS report as of 4/17/24 that has two transactions that were posted to help clear up an unbalanced in-process reconciliation report. There was a difference of \$1,203.32 and \$319.38 between the OST and Agency. The AFRS report shows that the cash was properly posted and the unbalanced amount is cleared. **No issues noted.**

### **Noted Weaknesses are as follows:**

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.6.PRГ - Long & Short Term Liabilities: Bonds**

*Procedure Step:* Key Control #2 - TM\$ (Manual)

*Prepared By:* JAG, 4/29/2024

*Reviewed By:* RKM, 6/18/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To confirm the process to record a bond sale and its associated receipt of funds (key control #2 for TM\$) in order to assess control risk.

**Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent

## State of Washington

material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.

## State of Washington

C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.

D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Key Control 2 - (Valuation, Completeness, and Classification)**

The Debt Program Analyst prepares tables for TM\$ based on the final numbers report package prepared by the state's municipal advisors. The Bond Program Manager reviews the tables for accuracy, and updates TM\$, which creates new bond payment amortization schedules. The Analyst then verifies the data imported into TM\$ by the Program Manager for accuracy and completeness against all originally prepared forms.

The understanding for this system is documented above in the "Controls - TM\$" step.

### **1. Confirmation of Key Manual Control:**

#### **Good Faith Deposit**

We reviewed a Cash Receipt (A8) for \$739,727,782.45 for VP GO Bonds (Taxable) Series 2024C, sold January 23, 2024. Leslie Yonkers, Debt Financial Officer, prepared and signed the A8 on 1/26/2024, Stephanie Richardson, COP Financial Analyst, approved/signed it on 1/30/2024, and validated in a batch process on 2/7/2024.

We reviewed the "TM\$ Update Worksheet" tables and tied to all other forms concluding all amounts and dates are in agreement. **No issues noted.**

We reviewed the TM\$ Update - "Bond Review Form" report for a new issue that was updated for the 2024D Bond sale on 2/6/24, and was reviewed on 2/28/24. The person who updated TM\$ was Austin Goble, Bond Program Manager, and Dawn Leopardo, Debt Program Analyst, reviewed the update in TM\$. **No issues noted.**

# State of Washington

## Noted Weaknesses are as follows:

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.6.PRG - Long & Short Term Liabilities: Bonds**

*Procedure Step:* Key Control #3 - TM\$ (Manual)

*Prepared By:* JAG, 4/29/2024

*Reviewed By:* RKM, 6/18/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm the debt service payment process (key control #3 for TM\$) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

## State of Washington

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

## **Key Control 3 - (Completeness and Valuation)**

To process monthly bond service payments, the Debt Financial Officer imports the CSV file from US Bank into TM\$ and runs a "TRE to US Bank" reconciliation report. The Officer pays the amount stated on US Bank's invoice unless the reconciliation identifies significant variances between the two sources. Typically the reconciliation shows a difference of only a few cents.

The understanding for this system is documented above in the "Controls - TM\$" step.

### **1. Confirmation of Key Manual Control:**

We reviewed the US Bank invoice dated 11/2/2023 for funds due 12/1/2023 and noted the following amounts:

Total principal due = \$36,515,351.80

Total interest due = \$56,058,109.77

Net amount due = \$92,573,461.57 (which totals the above figures)

We reviewed the December 2023 "Reconciliation Between Fiscal Agent and TRE Payments - All Records" report from TM\$ for the debt payment and noted the following amounts:

Fiscal Agent:

Total Debt Service: Principal = \$36,515,351.80

Total Debt Service: Interest = \$56,058,109.77

Total Debt Service = \$92,573,461.57

OST:

Total Debt Service: Principal = \$15,066,533.00

Total Debt Service: Interest = \$77,506,928.56

Total Debt Service = \$92,573,461.56

The reconciliation established that there was a \$0.01 difference in total debt service between the Fiscal Agent and OST. We reviewed the "DS Payment to US Bank" report prepared by Leslie Yonkers, Debt Financial Officer, reviewed by Stephanie Richardson, COP Financial Analyst, and signed and approved on 11/14/23. This report shows the Officer paid the amount stated on the US Bank invoice and shows TRE paid the extra penny. All of the supporting TM\$ report amounts and US Bank Invoice were in agreement of the reconciliation. **No issues noted.**

**Auditor's Note:** The way US Bank records zero coupon bond payments as principal and how TRE calculates the portion of payment as attributable to interest has resulted in differences with the principal or interest in prior audit periods.



# State of Washington

## Noted Weaknesses are as follows:

None

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **I.6.PR.G - Long & Short Term Liabilities: Bonds**

*Procedure Step:* Key Control #4 - TM\$ (Manual)

*Prepared By:* JAG, 6/18/2024

*Reviewed By:* RKM, 6/18/2024

Purpose/Conclusion:

#### **Purpose:**

To confirm the reclassification process of long-term liabilities (due within one year) (key control #4 for TM\$) in order to assess control risk.

#### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented*

## State of Washington

*key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

Record of Work Done:

## **Key Control 4 - (Completeness and Classification)**

The Debt Financial Officer prepares all of the monthly transactions in TM\$ (refunding, debt service payments, etc.) that are related to the calculation of the current bond payments which effects the long-term liabilities (due within one year) and long-term liabilities (due in more than one year). The Officer prepares the batches in TM\$ for the reconciliation to AFRS and the COP Financial Analyst reviews and approves them. This reconciliation to AFRS ensures that the amount in AFRS the long-term liabilities (due within one year) and long-term liabilities (due in more than one year) matches the amortization schedules in TM\$ for all bond issues. Once approved, TM\$ releases the batch and operations uploads them into AFRS as a part of end-of-day processing. The Officer receives the "In Process Report" (exception report) on the following day which she uses to ensure that all transactions posted properly in AFRS. The exception report runs every morning and only provides exceptions if an error occurs.

The understanding for this system is documented above in the "Controls - TM\$" step.

### **1. Confirmation of Key Manual Control:**

We reviewed the reconciliation for the month of March 2024. The reconciliation includes the following balances from TM\$ and AFRS:

#### **TM\$:**

GO Bonds, GL 5161 and 5261:	\$21,710,305,000.00
Revenue Bonds, GL 5162 and 5262	\$335,538,970.67
Proprietary, Remaining proprietary debt matured in FY2016	\$ 0
Zero Coupon, GL 5164 & 5264	\$150,977,373.30
Other Bonds Payable, GL 5169 & 5269	\$ 0
Total	\$22,196,821,343.97

#### **AFRS:**

GO Bonds, GL 5161 & 5261:	\$21,710,305,000.00
Revenue Bonds, GL 5162 & 5262	\$334,349,066.67
Proprietary, Remaining proprietary debt matured in FY2016	\$ 0
Zero Coupon, GL 5164 & 5264	\$150,977,373.30
Other Bonds Payable, GL 5169 & 5269	\$ 0
Total	\$22,195,631,439.97

The variance is due to TIFIA prepayment made on 12/1/2023. TM\$ has not been updated yet because OST has not received an updated debt service schedule from the Federal Government.

# State of Washington

The reconciliation included the following notes:

GL 5269 includes bonds for the Dairy and Fruit Commissions in Fund 999. The two funds are not in AFRS and the totals will not roll up properly unless they are reported in Fund 999. All amounts recorded in TM\$ matched AFRS. **No issues noted.**

ACFR figures are reported in the MD&A. Proprietary debt is reported as Business-Type activity.

GARVEE Bonds are recorded in TM\$ as limited obligation bonds. In AFRS, the liability is posted in GL 5262 Revenue Bonds Payable.

We tied amounts from the reconciliation (above) to the "ACFR-Outstanding by Disclosure Code and Fiscal Year" report for each bond type. We also tied the "Bond Retirement and Interest" report (CAF002) from AFRS to the above excel reconciliation by GL without exception. **No issues noted.**

We reviewed the "Bond Retirement and Interest" report (GL01) from AFRS to identify any early bond retirements and JVs related to the adjustments. There were no adjustments required for this year, and there are no associated JVs. **No issues noted.**

## **Noted Weaknesses are as follows:**

None

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control:**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **I.6.PR.G - Long & Short Term Liabilities: Bonds**

*Procedure Step:* Risk Assessment

*Prepared By:* JAG, 5/6/2024

*Reviewed By:* RKM, 6/18/2024

Purpose/Conclusion:
---------------------

# State of Washington

## **Purpose / Conclusion:**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

## Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

1. Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to a material misstatement ("total threat", which includes both naturally inherent risk and risk indicators), assuming that there are no related controls. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

## State of Washington

*Are there substantial pressures or motivations to misstate the balance?*

*Inherent Risk due to Misappropriation*

*· Is the account balance or transaction class susceptible to sizable misappropriation?*

*Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

2. Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and testing (if applicable). If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat). Note: control risk and inherent risk must be assessed separately and cannot be combined.*

*In order to set control risk to LOW, general controls would also need to be tested to provide evidence of the consistent operation of automated controls or automated controls would need to be sampled or tested throughout the audit period. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body.*

***All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

3. Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement is a combination of the auditor's separate assessment of inherent and control risk.

In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).

## State of Washington

When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

4. Design a substantive testing strategy that addresses the relevant assertion in all significant transaction streams included within the material line item.

*In addition to identifying what to audit (material balances) and what to audit for (relevant assertions), planning has also identified how much to audit (risk of material misstatement). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

**Completeness: High**

**Valuation: High**

**Classification: High**



# State of Washington

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**TM\$ - Completeness - Max:** For the risk that all bond payable amounts occurring during the period are not identified and recorded, we noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

**TM\$ - Valuation - Max:** For the risk that Bonds Payable amounts are reported at incorrect amounts, we noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

**TM\$ - Classification - Max:** For the risk that Bonds are not correctly classified between short and long term, we noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**TM\$ - Completeness - High**

**TM\$ - Valuation - High**

**TM\$ - Classification - High**

## **(4) Testing Strategy:**

Based on our assessment of the risk of material misstatement, we plan to perform the following tests:

### Valuation:

In order to determine if this line item is valued correctly, we will:

Reconcile the amounts recorded with the bond fiscal agent (U.S. Bank) to TM\$.

Review the year-end reconciliation completed by Leslie Yonkers, OST Debt Financial Officer.

Test the outstanding debt to ensure it is correctly recorded at year-end.

### Completeness:

In order to determine if this line item is complete, we will:

Confirm the balance at fiscal year-end to ensure bond sales were correctly recorded.

## State of Washington

Identify debt issued in FY24 and reconcile to AFRS to ensure all debt issued in FY24 was recorded. To do this, we will use the Electronic Municipal Market Access (EMMA) website which records all debt issued by state and local governments. It is funded and operated by the Municipal Securities Rulemaking Board and is designated by the U.S. Securities and Exchange Commission as the official source for municipal securities data and disclosures.

### Classification:

Reconcile the maturity dates with the bond fiscal agent (U.S. Bank) to TM\$.

Review the year-end reconciliation completed by Leslie Yonkers, OST Debt Financial Officer.

Test the outstanding debt to ensure amounts were properly classified between "Due Within One Year" and "Due in More Than One Year."

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### I.6.PRG - Long & Short Term Liabilities: Bonds

*Procedure Step:* Substantive Testing

*Prepared By:* JAG, 10/1/2024

*Reviewed By:* RKM, 10/17/2024

Purpose/Conclusion.
---------------------

### **Purpose:**

To determine whether all current & non-current liabilities as of the end of the period were reported (Completeness).

To determine whether current & non-current liabilities were reported at properly valued or calculated amounts (Valuation).

To determine whether financial statements properly classify current & non-current liabilities: bonds in conformity with generally accepted accounting principles (GAAP) (Classification).

### **Source:**

Leslie Yonkers, TRE Debt Financial Officer

### **Conclusion:**

We determined that all current & non-current liabilities as of the end of the period were reported (Completeness).

## State of Washington

We determined that current & non-current liabilities were reported at properly valued or calculated amounts (Valuation).  
We determined that financial statements properly classify current & non-current liabilities: bonds in conformity with GAAP (Classification).  
***No issues noted.***

### Testing Strategy:

The following is a list of **considerations** for testing the completeness assertion for current liabilities. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

For accruals resulting from normal operations (such as payroll or accounts payable), compare the accrued amount to prior years or to 1/12th of the total expenditure for the year to determine reasonableness. Follow-up as necessary to determine if all such expenditures were reported.

Inquire with AP clerks regarding invoices held, but not entered as of year-end (ie: due to pending litigation or disputes).

Obtain an attorney's letter or equivalent evidence regarding possible legal obligations of the entity. *Note: this test also gives evidence regarding rights & obligations.*

Review for compliance violations that would result in likely repayments. *Note: this test also gives evidence regarding rights & obligations.*

For governmental funds, compare current liabilities reported on the government-wide statements to those reported on the governmental funds balance sheet and verify that any differences are valid.

### Cut-off

Scan expenditure transactions recorded 1-3 months after fiscal year end to and test selected or sampled expenditures to determine if they were reported in the correct period.

-----  
The following is a list of **considerations** for testing the valuation assertion for current liabilities. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

*For current portions of long-term liabilities, see the valuation testing strategy for non-current liabilities. The same strategies can be applied to the entire liability, covering both current and non-current portions.*

Recalculate or review entity calculations of accruals (such as withholding taxes, accrued payroll, payroll taxes, accrued interest payable, etc).

-----  
The following is a list of **considerations** for testing the classification assertion for current liabilities. Results from planning procedures (inherent

## State of Washington

and control risk assessments) are the basis for the auditor's design of substantive tests.

Review supporting documentation to determine whether current liabilities are properly classified to the correct opinion unit.

Trace amounts due in within one year per debt-repayment schedules to check that it was properly shown as a current liability. Note that lines of credit and demand debt (debt that is payable at any time upon demand of the holder) should be classified as a current liability.

-----  
The following is a list of **considerations** for testing the rights and obligations assertion for current liabilities. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Determine whether the entity had legal authority to incur the liability.

Determine whether selected accruals are the obligation of the entity through review of source documentation.

Obtain an attorney's letter or equivalent evidence regarding possible legal obligations of the entity. *Note: this test also gives evidence regarding completeness.*

Review for compliance violations that would result in likely repayments. *Note: this test also gives evidence regarding completeness.*

### **Liabilities related to Joint Ventures or Other Arrangements**

Review forming documents and agreements to verify liability for current obligations of the venture.

Guidance/Criteria.
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Certificate of Participation (COP) Confirmations** (*applies to state agencies, including community colleges and universities*) - listing of outstanding COP debt at fiscal year end obtained directly from the State Treasurer

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS 3.4.1 Leases** - includes accounting procedures applicable to municipal leases

**BARS 3.4.4 Refunding Debt**

# State of Washington

## **BARS [3.4.9](#) Risk Management Principles**

## **BARS [3.4.15](#) Legal and Other Contingencies**

### **ADDITIONAL BACKGROUND**

-----  
Auditors should consider the following background information and resources when performing work on this area.

#### **Expenditure & Liability Recognition under Modified Accrual (Governmental Funds)**

Discussion of when an expenditure and, if payment is deferred, the respective liability should be reported under the modified accrual basis of accounting is described in GASB Interpretation 6 paragraphs 9-12.

"Matured liabilities ... should be reported as governmental fund liabilities. Matured liabilities include:

- a. Liabilities that normally are due and payable in full when incurred
- b. The matured portion of general long-term indebtedness (the portion that has come due for payment).

... Governmental fund liabilities and expenditures that should be accrued include liabilities that, once incurred, normally are paid in a timely manner and in full from current financial resources-for example, salaries, professional services, supplies, utilities, and travel. To the extent not paid, such liabilities generally represent claims against current financial resources and should be reported as governmental fund liabilities."

**Certificate of Participation (COP) Confirmations** (*applies to state agencies, including community colleges and universities*) - listing of outstanding COP debt at fiscal year end obtained directly from the State Treasurer

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.4.1](#) Leases** - includes accounting procedures applicable to municipal leases

**BARS [3.4.4](#) Refunding Debt**

**BARS [3.4.9](#) Risk Management Principles**

**BARS [3.4.15](#) Legal and Other Contingencies**

-----

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **Current & Non-Current (Government-wide and Proprietary Statements)**

GASB 34 paragraph 31 defines "current" versus "non-current" classification for liabilities:

"Governments are encouraged to present assets and liabilities in order of their relative liquidity. An asset's liquidity should be determined by how readily it is expected to be converted to cash and whether restrictions limit the government's ability to use the resources. A liability's liquidity is based on its maturity, or when cash is expected to be used to liquidate it. The liquidity of an asset or liability may be determined by assessing the average liquidity of the class of assets or liabilities to which it belongs, even though individual balances may be significantly more or less liquid than others in the same class and some items may have both current and long-term elements. Liabilities whose average maturities are greater than one year should be reported in two components—the amount due within one year and the amount due in more than one year..."

**Certificate of Participation (COP) Confirmations** *(applies to state agencies, including community colleges and universities)* - listing of outstanding COP debt at fiscal year end obtained directly from the State Treasurer

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS 3.4.1 Leases** - includes accounting procedures applicable to municipal leases

**BARS 3.4.4 Refunding Debt**

**BARS 3.4.9 Risk Management Principles**

**BARS 3.4.15 Legal and Other Contingencies**

-----  
**ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Certificate of Participation (COP) Confirmations** *(applies to state agencies, including community colleges and universities)* - listing of outstanding COP debt at fiscal year end obtained directly from the State Treasurer

# State of Washington

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.4.1](#) Leases** - includes accounting procedures applicable to municipal leases

**BARS [3.4.4](#) Refunding Debt**

**BARS [3.4.9](#) Risk Management Principles**

**BARS [3.4.15](#) Legal and Other Contingencies**

Record of Work Done.

### **Overview:**

We recorded our document request here [[Bond Testing Request](#)] which we used to obtain all documents required for testing.

### **Substantive tests performed to meet the Completeness assertion:**

#### **1. Identify debt issued in FY24 and reconcile to AFRS to ensure all debt issued in FY24 was recorded.**

We reviewed the Office of the State Treasurer website at [[Bond and COP Sale Results | Office of the Washington State Treasurer](#)] to determine what bonds were issued during FY 2024. The state exclusively uses EMMA's issuer page platform for all financial disclosures and official statements. We reviewed the official statements posted on the EMMA website and identified the bonds issued in FY 2024, see [[2024 Bond Testing](#)], tab "FY24 Bonds Issued". We obtained the bond closing memorandums, A8 cash receipts, and good faith deposit journal summaries for each bond sale from Leslie Yonkers, Debt Financial Officer. We tied the closing memorandums to the bond sales posted on the EMMA website and recalculated the net bond proceeds. We compared the recalculated net bond proceeds for each bond series to the total deposit on the A8 cash journal summaries. **No issues noted.**

We ran a query in the AFRS database for bond proceeds at [[2024 Bond Testing](#)], see tab "FY24 Bonds Issued," beginning on row 38. The query includes Income Statement Sort Codes ND (Bonds Issued) and NH (Issuance Premiums). We used the par values and the associated discount/premium amounts from the closing letters to recalculate bond proceeds as noted above. We then compared the calculated totals to the bond proceeds recorded in AFRS without exception. **No issues noted.**

#### **2. Confirm the balance at fiscal year-end to ensure bond sales were correctly recorded.**

We ran a query in the AFRS database at [[2024 Bond Testing](#)], see tab "ACFR Query", for the outstanding bond debt reported in the General Long-Term Obligations fund. We noted a total of \$20,752,338,224.13 after excluding accreted interest payable (\$213,445,282.76) and excluding fees payable (\$184,987.70). We added the portion moved to short term, excluding COP, in the amount of \$1,236,882,978.08 for a total of

## State of Washington

\$21,989,221,202.21 recorded in AFRS. We tied the total recorded in AFRS to the total bonds on the TM\$ report. We determined that the long term liabilities: due within one year and due in more than one year are properly recorded. **No issues noted.**

### **Substantive tests performed to meet the Valuation assertion:**

#### **1. Review the year-end reconciliation completed by Leslie Yonkers, TRE Debt Financial Officer.**

We obtained the 6/30/2024 TRE Bond reconciliation spreadsheet from Leslie and noted that a reconciliation was performed between the Treasury Management System and the bond fiscal agent, US Bank. Additionally, we re-performed the reconciliation [[2024 Bond Testing](#)] as noted below and found no variances between our reconciliation and the reconciliation performed by Leslie Yonkers. **No issues noted.**

#### **2. Test outstanding debt and reconcile the amounts recorded with the bond fiscal agent (U.S. Bank) to TM\$ to ensure it is correctly recorded at year end.**

We obtained and reviewed the outstanding bond debt report created by the Treasury Management System ("Loan Accounts List- for Outstanding Bonds - Series"). We also obtained the US Bank confirmation report that showed outstanding bonds and included defeased bonds, see [[2024 Bond Testing](#)], tab "USBank Confirmation." Defeased bonds are in escrow and are appropriately excluded from the TM\$ balance as they are no longer a liability of the State. We reviewed communication between Leslie Yonkers and US bank to determine there were no defeased bonds during FY24. Additionally, Leslie Yonkers provided us with a Zero Coupon bonds outstanding spreadsheet, see [[2024 Bond Testing](#)], tab "Zero Coupon Bonds." The spreadsheet provides a breakdown of the interest and principal for the zero coupon bonds. We tied the principal for the zero coupon bonds to the TM\$ outstanding column and the total debt service column amounts to the US Bank outstanding balances.

We re-performed the reconciliation between the outstanding bond debt report created by the Treasury Management System and the US Bank confirmation report at [[2024 Bond Testing](#)], see tab "Bond Confirmation." We tied the outstanding principal from the TM\$ report to the outstanding principal from the US Bank confirmation (less refunded bonds and the zero coupon bond difference). We tied the zero coupon bond differences between the TM\$ report and the US bank confirmation to the zero coupon bond interest. We noted a difference between the TM\$ report and the US Bank confirmation in the amount of (\$15,089,701). We determined this difference was related to the WASTIF13C- Toll Revenue Bond. We discussed this with Leslie Yonkers, TRE Debt Financial Officer, who stated that there is a variance for the TIFIA bonds because they are only authorized to issue \$300,000,000 and interest accrued before any debt service payments are made. US Bank and TRE record these differently. US Bank adds the accrued amounts to the principal and TRE adds it to the interest. We reviewed the "TIFIA - SR 520" spreadsheet, that has the calculated ending balance of loan amortization schedule and annual projected payments, and the "TIFIA OST and US Bank Variance FY2024" spreadsheet, used to verify US Bank's ending principal balance and TRE's ending principal balance since they differ. Both TIFIA spreadsheets were obtained from Leslie Yonkers and we noted that the accrued interest on the debt service schedule tied to the difference between the TM\$ report and the US Bank confirmation. **No issues noted.**

### **Substantive tests performed to meet the Classification assertion:**

#### **1. Reconcile the maturity dates with the bond fiscal agent (U.S. Bank) to TM\$.**

We obtained the 6/30/2024 TRE Bond reconciliation spreadsheet of the reclassification of long-term to short-term FY ending 6/30/24 from Leslie



# State of Washington

Yonkers, TRE Debt Financial Officer and noted that the reconciliation was performed between the Treasury Management System and the bond fiscal agent, US Bank. We noted that each bond within the reconciliation had matching maturity dates between TM\$ and US Bank. **No issues noted.**

## **2. Review the year-end reconciliation completed by Leslie Yonkers, TRE Debt Financial Officer.**

We obtained the 6/30/2024 TRE Bond reconciliation spreadsheet of the reclassification of long-term to short-term FY ending 6/30/24 from Leslie Yonkers, TRE Debt Financial Officer and noted that the reconciliation was performed between the Treasury Management System and the bond fiscal agent, US Bank. Additionally, we re-performed the reconciliation as noted below and found no variances between our reconciliation and the reconciliation performed by Leslie Yonkers. **No issues noted.**

## **3. Test the outstanding debt to ensure amounts were properly classified between "Due Within One Year" and "Due in More Than One Year."**

We obtained TM\$ reports "Debt Service Payments - for a Month Detail" for all fiscal months in which TRE plans to pay bonds in FY25 (due within the next fiscal year) from Leslie Yonkers, TRE Debt Financial Officer. Using the TM\$ reports, we identified and summed the debt service principal payments due by 06/30/2025 between general obligation bonds, revenue bonds, and zero coupon bonds for each month at [2024 Bond Testing], see tab "Classification." Using the US Bank confirmations report, see tab "USBank Confirmation, [2024 Bond Testing]" we calculated the total amounts outstanding for the three bond types. We reduced the US Bank confirmation total outstanding with the TM\$'s principal payments due by 6/30/2025 to come to a recalculation of the long-term debt portion - "Due in More Than One Year." We had to make additional adjustments for the recalculation of the revenue and zero coupon bonds. The revenue bonds required an adjustment of \$15,089,701, see at [2024 Bond Testing], for the accrued interest of the WASTIF13C- Toll Revenue Bond. The zero coupon bonds required an adjustment of \$336,286,603, see at [2024 Bond Testing], for the zero coupon bond interest contained within the US Bank confirmation report. We then compared both the principal payments due by 6/30/2025 ("Due Within One Year") and the recalculated long-term debt ("Due in More Than One Year") to the amounts reported on the AFRS database, see tab "ACFR Query," and noted no variances at [2024 Bond Testing], see tab "Classification." We determined FY24 bonds are correctly classified between "Due Within One Year" and "Due in More Than One Year." **No issues noted.**

## **I.7.PR.G - Paid Family & Medical Leave - Expenses**

*Procedure Step:* Summary & Conclusion

*Prepared By:* JLE, 10/4/2024

*Reviewed By:* RKM, 11/21/2024

# State of Washington

Purpose/Conclusion:

## **Purpose**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

## **Conclusion**

We determined that **no modifications were necessary** to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

## **Information to be used as audit evidence:**

Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?

## State of Washington

- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

### Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
  - Did tests identify a different level or type of risk than the planned audit response was designed to address?
  - If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

# State of Washington

## SAO Audit Policy [3210](#) – Audit Evidence

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

**(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

**(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### I.7.PRГ - Paid Family & Medical Leave - Expenses

*Procedure Step:* Understanding of Line Item

*Prepared By:* JLE, 6/4/2024

*Reviewed By:* SHW, 7/10/2024

Purpose/Conclusion:

**Purpose / Conclusion**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

**STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

**STEP 2: Analyze Composition and Changes of Line Item**

## State of Washington

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

# State of Washington

Guidance/Criteria:

Record of Work Done:

## **(1) Prior Audit Exceptions**

Paid Family & Medical Leave (PFML) was not tested in prior-year Annual Comprehensive Financial Report (ACFR) audits. In the FY22 Employment Security Department (ESD) accountability audit, we issued a finding relating to inadequate controls over the PFML program. Specifically, we found:

- ESD had not implemented controls to prevent claimants from receiving PFML benefits in the same claim week where they are receiving unemployment (UI) benefits, resulting in \$1M of improper PFML expenditures.

- ESD had not implemented processes or procedures to assess and collect PFML penalties or overpayments, as required by State law.

Per inquiry on 5/16/2024 with Eric West (ESD PFML Fraud Manager), John Mattes (ESD PFML Operations Manager), and Shalina Latiff (ESD PFML Program Manager), we found that while ESD has implemented controls to help detect double-payments made between the UI and PFML programs, the agency has not yet implemented preventative controls. Currently, the main preventative control is a question within the online weekly claim portal, which asks claimants whether they received UI benefits for the week. Additionally, ESD has not yet implemented processes or procedures to collect PFML-related penalties or overpayments.

**We reviewed the amount of double-payments made between the UI and PFML programs for FY23, noting that such payments are insignificant to the ACFR; as such, we will not include these double-payments in our testing strategy for PFML at the State-wide level.** These prior accountability audit exceptions will be followed up on in the FY23 accountability audit at TM file: *S1-EmploymentSecurity-AC23*.

## **(2) Composition & Change Analysis**

See Line Item Leadsheet at: [\[Line Item Lead Sheet\]](#).

ESD considers PFML expenditures to be direct payments to program claimants, as well as those ancillary costs necessary to implement and support the PFML program. We analyzed the expenditure amounts at the line item lead sheet and identified SubObject NA 'Direct Payments to Clients' as significant, comprising 95% of total FY23 balance expenditures.

We note that there was a 49% increase between FY22 and FY23 expenditures. Per ESD's [FY23 Actuarial Annual Report](#) for PFML (ref: page 7), we found that this change was primarily caused by both an increase in the average weekly benefit amount awarded, as well as in the number of claims submitted year-over-year.

## State of Washington

We analyzed the PFML Claims Dashboard located at: <https://esd.wa.gov/labormarketinfo/paidleave/claims-data>, noting the following:

The average weekly benefit amount increased from \$891 in FY22 to \$957 in FY23 (7.5% increase).

The number of family and medical claims submitted increased from 212,164 in FY22 to 245,795 in FY23 (16% increase).

There were 1,365,795 of compensated weeks paid in FY22, and 1,578,233 weeks compensated in FY23 (15.5% increase).

The number of individuals choosing to participate in elective PFML coverage increased from 1,079 to 1,235 from FY22 to FY23 (14.5% increase).

**Overall, we identified no unusual or unexpected elements that may indicate unidentified areas of risk for PFML expenditures.**

### Additional Background: Program Information

The PFML program is made up of two claimant categories: medical leave and family leave. Benefits are paid at a rate of up to 90% of a worker's average weekly pay.

Medical leave is provided for an individual's personal health condition (e.g., surgery, pregnancy, mental health, chronic conditions, or inpatient treatment); claimants may receive up to 12 weeks\* of leave per claim year\*\*.

Family leave is provided to assist with a relative's serious health condition, for bonding with newly born/adopted children, and for military family leave relating to deployments; up to 12 weeks\* of leave per claim year\*\*.

*\* If an individual has more than one qualifying event in the same claim year, they may receive up to 16 weeks of combined family/medical leave. If an individual experiences a condition in pregnancy which results in incapacity, they may receive up to 18 weeks of combined family/medical leave.*

*\*\* The claim year begins on the Sunday of the week in which a worker submits an initial application, and expires 52 weeks later.*

Leave does not have to be taken all at once; however, workers must claim a minimum of 8 consecutive hours of leave each week. Regardless of how a worker takes their leave, they must file a claim every week (including during the waiting week). Workers cannot take medical leave and family leave in the same week, nor can they collect unemployment or worker's compensation during the same week that they collect PFML benefits. Additionally, any employer-provided paid time off should be reported in the weekly claim, and will reduce PFML benefit payments for that week.

The waiting week is the first week in which a worker is approved to file a claim and use leave. Generally, workers are not paid for the waiting week period. Exceptions include parental bonding leave, medical leave taken during the postnatal period, and military exigency. A week is defined as Sunday through Saturday; as such, if a qualifying event occurs on a weekday, then the waiting week may be less than 7 days. During this waiting period, workers may use paid time off from employers without impacting their PFML benefits.

In order to qualify for the program, a worker must have worked a minimum of 820 hours in Washington State during their qualifying period. The qualifying period is normally defined as the first four of the last five completed calendar quarters, or, the last four completed calendar quarters immediately preceding the application for leave. The 820 hours can be counted for full-time, part-time, temporary, or seasonal work; additionally,

## State of Washington

the work hours can be counted in situations where an individual works multiple jobs for different employers, or when an individual switches employers.

Program exemptions include: federal employees, employees of tribally-owned businesses on tribal land, self-employed persons or independent contractors (unless they've opted-in for elective coverage), or workers covered by an employer's voluntary plan.

### **(3) Updates to Significant Account Matrix**

We updated the relevant accounting systems to include the OMAC Portal and Microsoft Dynamics.

### **I.7.PRG - Paid Family & Medical Leave - Expenses**

*Procedure Step:* Controls - OMAC Portal & Dynamics

*Prepared By:* JLE, 7/2/2024

*Reviewed By:* SHW, 11/4/2024

Purpose/Conclusion:

#### **Purpose**

To gain an understanding of internal controls within the OMAC Portal and Microsoft Dynamics systems used by ESD; relevant to the rights and obligations, valuation, and completeness assertions.

#### **Conclusion**

We gained an understanding of internal controls as documented in the record of work done.

We noted the following control weaknesses, which we **do not** consider to represent significant deficiencies or material weaknesses:

**Control Weakness 1** - PFML claim adjudicators have the ability to manually adjust/override system-calculated benefit amounts; there is no secondary review performed over such manual adjustments. **See issue at:** [E: ESD PFML Control Weaknesses].

**Control Weakness 2** - ESD has not implemented detective controls to identify multiple payments made to a single claimant between the PFML and workers' compensation benefit programs. **See issue at:** [E: ESD PFML Control Weaknesses].

Testing Strategy:

**The following procedures are required for all material systems:**



## State of Washington

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

## State of Washington

Who or what initiates the control

When (or how often) is the control applied

Who performs the control

As needed, the experience, knowledge and attitude of the person applying the control

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any exceptions or alternative processing to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

[Financial Statement Audits](#) Planning Guide

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

Internal controls address the following balance:

Paid Family & Medical Leave Compensation (Expenses)

For the following assertions:

Rights and Obligations - There is a risk that ineligible claimants were improperly approved for benefits.

Valuation - There is a risk that benefit amounts paid were not accurately calculated based on claimant wages and hours worked during the qualifying period.

Completeness - There is a risk that the year-end actuarial accrual amount for claims payable used unreasonable estimation methodology or source data. There is a risk that balances reported between Microsoft Dynamics and AFRS are incomplete.

## **Gain an Understanding of Internal Controls**

We gained an understanding of internal controls over PFML claim expenditures as follows:

Meeting with Steve Zawoysky (Leave and Care Division Treasury Manager) and Mary Turpin (Chief Financial Accountant) on 4/25/2024.

Meeting with John Mattes (Leave and Care Operations Manager) and Rob Rohrer (PFML Customer Service Manager) on 4/30/2024.

Meeting with Imran Shaik (Leave and Care Developer), Bora Kim (Application Developer), Bryon Schabell (Application Quality Assurance Supervisor), and Jeanette Ritchie (Leave and Care Product Manager) on 7/9/2024.

## **Filing a New Claim**

The majority of PFML claimants file their initial benefits application through the external OMAC online portal (the Portal), located at:

[secureaccess.wa.gov](https://secureaccess.wa.gov). Applicants must go through Secure Access Washington multi-factor authentication steps to access the Portal. In cases where a paper application is received, a customer care specialist will enter information into the Portal on the claimant's behalf.

The application requires several fields relating to personal and contact information (phone number, email address, street address, SSN, first and

## State of Washington

last name), demographic information (gender, ethnicity/race), and employment history. The application also guides users through several sets of questions, designed to ensure adherence to the provisions of the program (e.g., 'Did you know you would need to take leave before your leave started?', and 'Did you notify your employer in advance that you needed leave?'). The application also includes user-friendly definitions; for example, the yes/no question 'Are you experiencing complications related to your pregnancy?' includes a pop-up definition box reading: "Complications can include severe morning sickness, prenatal complications resulting in bedrest, pre-eclampsia, infections, or other prenatal complications." Finally, the Portal requires claimants to upload documentation supporting their application. A list of acceptable documentation can be found at: [paidleave.wa.gov/library](https://paidleave.wa.gov/library).

Once an application is received, ESD's customer relationship management software (CRM) automatically queues all applications in the order in which they were received, and assigns them to adjudicators. All applications are reviewed by an adjudicator to determine eligibility, prior to issuing an approval or denial decision for benefits (**Key Control 1 - Rights & Obligations**). The eligibility decision is documented in all cases by using standardized case template notes, which includes the adjudicator's name and a description of what verification and fact-finding steps were performed. Adjudicators receive a formal training process, which lasts approximately one year. During the training period, adjudicators work through applications under supervision and all work performed by an adjudicator-trainee receives a secondary review by a journey-level adjudicator. After completing a year of training, qualified adjudicator-trainees are promoted to 'Adjudicating Specialist 2', and are allowed to adjudicate claims independently.

When reviewing an application, adjudicators perform the following steps:

### **Verifies ID documentation provided by the applicant**

We reviewed ESD Policy 2.415 'Discrepancies Between ID Documents and Applicants Name'. Adjudicators are required to verify claimant identity by comparing information provided on the application to the claimant's ID document. There are varying levels of identification required to be performed, each dependent on a variety of scenarios. If a claimant's full name matches exactly between the two documents, then no additional fact finding is needed. If a claimant's name is a close match (e.g., multiple last names on ID, but one last name in CRM, or Matthew Jones vs. Matt Jones), then the date of birth must also be verified. If two different names are provided, then additional fact finding must be performed for government-issued documentation which shows the change from one name to another. In all cases where the two names are not an exact match, then the adjudicator will make a note of their findings about the claimant's name in the 'Remarks' section of the *Benefit Claim Decision* case note.

### **Verifies applicant eligibility for benefits by:**

#### **Reviewing hours and wages reported by for the applicant by their employer**

#### **Determining whether a qualifying event occurred under [RCW Title 50A](#)**

To verify eligibility, adjudicators review information within the application, as well as supporting documentation uploaded to the Portal. Per ESD Policy 2.439 'Fact-Finding Procedure', if there is not enough information to determine eligibility for benefits, adjudicators are required to perform fact-finding. Fact-finding consists of (at minimum) two contact attempts, using two different methods, prior to making an adjudicative decision. All fact-finding attempts, responses, and outcomes (including copies of letters) must be recorded and attached in

## State of Washington

the case's *Timeline*, and as a *Fact-finding* case note.

To verify hours and wages reported by the employer, the adjudicator first identifies the qualifying period, based on the application date. Then, they review information in the *Wage Search* page, determining whether reported information appears complete and correct. If information appears to be missing or incorrect, the adjudicator is required to contact both the claimant and employer to perform additional fact-finding.

To determine whether a qualifying event occurred under RCW Title 50A, the adjudicator may accept one of the following forms of documentation:

- FMLA Designation Notice (i.e., approval letter) paired with an FMLA medical certification

- Written documentation from the employer, that they accept the certification of a serious healthcare condition from the healthcare provider in question

- A certification form with an authorized provider's signature

- An Explanation of Benefits showing that the chosen healthcare provider is covered under the employer's group health plan

- Documentation of birth or adoption, showing the name of the claimant as the parent

- Documentation showing military deployment or leave, including applicable dates

### **Enters the approved leave starting and ending dates, and generates an approval letter to the claimant**

After reviewing applicable documentation, adjudicators are responsible for manually setting the applicable start and end dates for the number of approved leave weeks within the Portal. They also generate and send an appropriate approval or denial letter, which is sent via U.S.P.S. to the applicant's address on file. A copy of the letter is maintained and uploaded to the Portal for recordkeeping.

### Calculating Benefits

Once an applicant has been approved for PFML benefits, they must submit weekly claims in order to continue collecting payments. Weekly claims are submitted online, in the same external OMAC Portal used for new applications. After filing a weekly claim, the Portal then automatically calculates payments via the Benefit Calculator Tool (**Key Control 2 - Automated Software Calculation - Valuation**). This tool relies on any manual information input by adjudicators during the application review, as well as cross-matched data from employer-submitted quarterly wage reports showing hours worked and employee salary information.

The weekly benefit amount is calculated based on a worker's average weekly wage, and the amount actually paid is then prorated based on a comparison of actual to average work week hours. It's important to note that these averages are calculated based on hours worked and wages earned during the qualifying period and are *not* based on a claimant's current work schedule or current earnings at the time of adjudication.

During our control meetings, we found that adjudicators have the ability to manually adjust/override the system-calculated benefit amount; there is no secondary review performed over such manual adjustments (**Control Weakness 1**).

# State of Washington

## *State Average Weekly Wage Determination*

The weekly benefit amount also takes into consideration the State's average weekly wage. The State average weekly and average annual wage is calculated annually by ESD's DATA division. The source data used for the average annual wage calculation is a computer-generated report within the unemployment (UI) data warehouse and is calculated by dividing the total wages reported by all employers by the average number of workers reported for all months of the year. The State's average weekly wage is then derived by dividing the average annual wage by 52, rounded down to the nearest dollar. For more information, see: [RCW 50.04.355](#).

## *Average Weekly Wage and Weekly Benefit Amount*

For more information, see: [WAC 192-610-051](#).

A worker's average weekly wage is established as follows: total reported wages in the claimant's two highest-paid quarters during the qualifying period is divided by 26, then rounded down to the nearest multiple of one dollar.

The weekly benefit amount is then calculated as follows:

If the worker's average weekly wage is less than or equal to 50% of the State's average weekly wage, then the weekly benefit amount will be 90% of the worker's average weekly wage.

If the worker's average weekly wage is greater than 50% of the State's average weekly wage, then the benefit amount is as follows:

90% of 1/2 of the State's average weekly wage, plus:

50% of the difference between 1/2 of the State's average weekly wage and the worker's average weekly wage.

## *Average Work Week Hours*

For more information, see: [WAC 192-610-050](#).

For salaried workers - typical work week hours are determined to be 40.

For all other workers - the system calculates using the sum of all hours reported during the qualifying period, divided by 52, then rounded down to the nearest hour.

## *Factors Affecting Weekly Benefit Amounts Actually Paid*

The weekly benefit is subject to minimum and maximum payment amounts; in FY24, these amounts were as follows:

CY23 (July 2023 - December 2023) - minimum benefit amount of \$100/week, maximum benefit amount of \$1,427/week.

CY24 (January 2024 - June 2024) - minimum benefit amount of \$100/week, maximum benefit amount of \$1,456/week.

The weekly benefit amount is reduced by the amount of employer-paid leave reported by the claimant for that given week (with the exception of the waiting week). As mentioned above in 'Calculating Benefits', the weekly benefit amount is also subject to proration by the number of actual hours claimed for PFML, relative to the workers' average work week hours. For example, assume that an employee has a weekly benefit amount of \$600:

## State of Washington

If an employee files a weekly claim for 40 hours of PFML, and their average work week hours are also determined to be 40 hours, then they will receive \$600 in benefits that week.

If an employee files a weekly claim for 20 hours of PFML, and their average work week hours are determined to be 40 hours, then they will receive \$300 in benefits that week ( $=(20/40)*600$ ).

A claimant is not eligible for PFML benefits to be paid if they report claiming unemployment or workers' compensation benefits in that same week; the system will automatically reduce the weekly benefit to zero in such cases. We note that prior to January 2023, ESD relied on claimant self-attestation to prevent 'double dipping' in multiple benefit programs. Beginning in January 2023, ESD implemented a cross-match between PFML and unemployment benefit (UI) data. Each week, the Leave and Care division sends a list of all new PFML claims captured in the prior week to the Data Analytic (DA) team. Team DA then adds UI data to the PFML claim spreadsheet, and utilizes a formula to identify cross-matches within the two populations, based on SSN and payment week. The results are then sent to the Fraud team for further investigation and follow-up. At this time, there are no detective controls in place to identify multiple payments made to a single claimant between the PFML and workers' compensation benefit programs (**Control Weakness 2**).

### **How Transactions are Recorded in AFRS:**

Weekly claims submitted through the Portal are automatically routed to Microsoft Dynamics via an overnight, automated upload process. During this automated process, claim information is entered in Dynamics as a vendor payment journal. Prior to posting in AFRS, PFML benefit expenditures go through two levels of review in the Dynamics system.

On a daily basis, Fiscal Analyst 3 (FA3)'s are tasked with downloading and preparing Dynamics payment journals, which summarize all claims approved and auto-uploaded from the preceding day, detailing where benefit payments will be routed. While preparing this report, the FA3s ensure that the journals present ACH payment totals separately, depending on whether the payment will route to a personal or a business account. After preparing these reports, the FA3 will mark the files as 'prepared' within Dynamics and the system will automatically route for a reviewer's approval.

ESD Treasury Department Leads perform the first level of review over pending benefit payments. During their review, the Lead performs fraud verification, ensuring that approved benefits correspond to valid, approved Portal accounts, and that the claimant is not included on an identity fraud list which is maintained by ESD's Compliance Division. Additionally, the Lead reviews that claimed weekly benefit amounts do not exceed the program's maximum weekly benefit amount, which was \$1,456/week in FY24. Finally, the Lead ensures that the payment journal totals are in agreement with claims filed via the Portal. Once this first review has been completed, the Lead indicates their approval electronically in Dynamics, and the payment file is routed to a Treasury Supervisor.

During the second level of review, the Treasury Supervisor will again ensure that Portal information ties out to the payment journals, that there are separate payment journals attached for each payment process (i.e., personal vs. business ACH routing destinations), that the total of each payment process type is accurate, and that the effective date is correct. Once complete, the Supervisor indicates their approval electronically in

## State of Washington

Dynamics. As a final approval indication, Steve Zawoysky (or, as backup, a Supervisor) will sign the transmittal register, and transmit the reviewed benefit payment information to the Treasury Management System (TMS), via a Managed File (MFT) drop. OST is responsible for maintaining TMS, which communicates with AFRS.

### AFRS Reconciliation

At the end of each month, Mary Turpin oversees as FA3's perform a reconciliation of information which was reported to AFRS via TMS, using 'Toolbox' software. First, staff runs a monthly summary of the Vendor Payment Journal in Dynamics, showing all monthly activity which was reported to AFRS. Then, they run the 'General Ledger Activity Flexible' WebI report in the Enterprise Reporting system for the same month, showing how AFRS is currently reporting the data for relevant GLs and funds; the coding for PFML benefit claims is Fund 22F, GLs 5118, 5190 and 6510. PFML benefit claims also hits cash accounts, which are coded as Fund 22F, GLs 1100, 7110, 7120, and 7140. The two amounts are compared for accuracy and completeness (**Key Control 3 - Valuation, Completeness**). Any adjustments needed, such as amounts which are missing a program designation, are completed via the Toolbox software and, as necessary, Form A7-A 'AFRS Journal Voucher'. After reconciling the data and preparing any adjustments, the FA3 will email an approver, requesting that the toolbox reconciliation be reviewed and released. This same process occurs again at year-end, for the entire fiscal years' reporting activity. Mary is responsible for reviewing and approving any year-end reconciliations and adjustments.

At year-end, Mary is also responsible for receiving an actuarial estimate regarding claims payable, and preparing a manual journal entry to record the accrual (**Key Control 4 - Completeness**). The estimate is comprised of two components: claims which have already been filed and have a remaining payable associated, as well as claims which have been incurred, but not yet been filed. The PFML Actuarial team completes the estimate using historical data compiled by the Data and Research team. The IBNR is measured using Actuarial Standard of Practice No. 43.

Significant assumptions relevant to the estimate are as follows:

- Employee wage growth by year
- Investment yield
- PRAD confidence level
- Expense ratio
- Wage seasonality
- UI rates
- Covered employee development factor
- Assessed premium development factor

For more information regarding the actuarial estimate, see: [\[Estimates List\]](#). After the PFML Actuary team completes their estimate, the amount is emailed to Mary after being approved in a 'go/no-go' meeting. Once Mary completes the accrual JV, her work is reviewed for accuracy by the PFML Actuary team, the Treasury Manager, and the Deputy CFO prior to posting. After year-end close, the accrual entry is then reversed at the beginning of the next fiscal year.



## State of Washington

### Key Controls are as Follows:

- Key Control 1 (Rights & Obligations)** - All PFML applications are reviewed for eligibility by an ESD adjudicator prior to issuing an approval or denial decision for benefits.
- Key Control 2 (Automated Software Calculation - Valuation)** - The external OMAC online portal automatically calculates weekly benefit payment amounts via the Benefit Calculator Tool.
- Key Control 3 (Valuation, Completeness)** - ESD Treasury staff perform a monthly reconciliation between AFRS and Dynamics, ensuring that amounts reported between the two systems are accurate and complete.
- Key Control 4 (Completeness)** - At year-end, the Chief Financial Accountant is responsible for preparing a manual journal entry to record an accrual for claims payable, based on actuarial estimates.

### Noted Weaknesses are as Follows:

- Control Weakness 1** - PFML claim adjudicators have the ability to manually adjust/override system-calculated benefit amounts; there is no secondary review performed over such manual adjustments.
- Control Weakness 2** - ESD has not implemented detective controls to identify multiple payments made to a single claimant between the PFML and workers' compensation benefit programs.

### I.7.PR.G - Paid Family & Medical Leave - Expenses

*Procedure Step:* Key Control 1 (Manual)

*Prepared By:* JLE, 6/21/2024

*Reviewed By:* SHW, 7/10/2024

Purpose/Conclusion.*
----------------------

#### **Purpose**

To confirm that all Paid Family and Medical Leave claim applications are reviewed for eligibility by an Employment Security Department adjudicator (**Key Control 1 for the OMAC Portal**), in order to assess control risk.

#### **Conclusion**

We noted **no** material weaknesses or significant deficiencies in internal controls. **No control weaknesses noted.**

# State of Washington

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified*

## State of Washington

*issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.365 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control 1 (Rights & Obligations): All PFML applications are reviewed for eligibility by an ESD adjudicator prior to issuing an approval or denial decision for benefits.**

The understanding for this system is documented above in the "Controls - OMAC Portal & Dynamics" step.

### **1. Confirmation of Key Manual Control**

We confirmed this key control through a live walkthrough demonstration with Jeannette Ritchie (Leave and Care Transformation Team Product Manager) and Eric Ayres (Leave and Care Service Delivery Manager), on 6/13/2024, as follows:

First, we reviewed the PFML Customer Care Team CRM System main page. Jeannette navigated to 'Service Cases' and entered case number FJS2YSKM0X-1, which pulled up a 'Benefits Claim - Portal' page. We noted the following case information from the Claim Summary:

The application was submitted by Janice Marie C Palacios (the claimant) on 6/3/2024.

Claimant's birthdate was listed as 1/22/1974.

As of 6/13/2024, the case status was 'Resolved' and the claim status was 'Approved'.

The claim type was identified as 'Medical', and the question Secondary Qualifying Event? was marked as 'Yes'. The claim sub-type was 'Self-Serious Medical Condition'.

Leave start date requested was 5/25/2024, and leave end date requested was 6/10/2024.

The effective start date and claim year start date was 5/19/2024, and the effective end date was 6/15/2024.

The qualifying period start date was 1/1/2023.

There were 2 employers automatically identified by the Portal (due to cross-match with employer quarterly wage reporting):

Infinity Global Distribution LLC and Barmor Temporaries, Inc.

Current employment status is hourly, or part-time salaried, employee.

There were no other employers manually added by the claimant.

## State of Washington

A case note was added on 6/13/2024 at 8:45AM by James Moses (ESD), specifically noting that the following was verified: proof of identity, claim year, hours worked in base qualifying period, claim type, and leave dates. The claim status was updated to 'Approved' per the case note.

Next, we reviewed 3 supporting documents uploaded by the claimant:

### Proof of Identity

The claimant submitted a State driver's license.

We note that the claimant's name and DOB match exactly to that which was submitted on their application.

We additionally note that the driver's license appears legitimate, and is unexpired.

### Medical Certification

The claimant utilized ESD's PFML Medical Certification template form.

The claimant name, DOB, and leave request dates match that per the application without exception.

The serious health condition was due to an emergency surgery needed.

The form was signed by the claimant's medical provider on 6/3/2024, and included their certified physician assistant license number, medical practice type (general surgery), and contact information.

### Other

The claimant submitted a copy of the written record which they provided their supervisor on 5/28/2024, stating their intent to take leave due to surgery, from 5/28/2024 - 6/10/2024.

Finally, we reviewed 'Wage Search' information, which displays quarterly wage report information submitted by employers via the Portal, cross-matched to the claimant's name and SSN:

We note that the summary from wage search displayed information relevant to the claim year start date of 5/19/2024 - the summary included wage reporting information for CY23 Q1 - CY24 Q1.

*Note - the qualifying period is the first four of the last five completed calendar quarters starting from the day the employee intends to take leave.*

The claimant worked 1,668 hours in CY23 Q1 - Q4, putting them well above the needed threshold of 820 hours in order to qualify for PFML leave.

We confirmed that the claimant's identity is valid (Step 2), that they experienced a qualifying medical event (Step 2), and that they worked sufficient hours in the qualifying period to qualify for PFML leave (Step 3). We additionally confirmed that this information was verified by an ESD adjudicator prior to application approval, as indicated in the case notes (Step 1). **No issues noted.**

**Noted Weaknesses are as Follows:**

# State of Washington

None noted.

## **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **3. Control Risk at LOW - Test Key Manual Control**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at '**MAX**'.

### **I.7.PRG - Paid Family & Medical Leave - Expenses**

*Procedure Step:* Key Control 2 (AUTOMATED)

*Prepared By:* JLE, 8/6/2024

*Reviewed By:* RKM, 8/13/2024

Purpose/Conclusion.:

#### **Purpose**

To determine whether the automatic calculation of weekly benefits (Key Control 2 for the OMAC Portal) was in place and operating effectively, and to consider related general IT controls, in order to assess control risk.

#### **Conclusion**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure the control operated consistently during the audit period; however, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented above in the "Controls - OMAC Portal & Dynamics" step.

Testing Strategy.:

The following procedures are **required** for all automated key controls for financial and single audits:

# State of Washington

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step.

Auditors should consider the following aspects of the automated control when gaining an understanding:

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control.

To test the automated control, consider the following procedures:

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source*

## State of Washington

*rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses.

Auditors should consider the following aspects of general IT controls when gaining an understanding:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*



## State of Washington

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW.

If general IT controls are tested, consider the following procedures:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

## State of Washington

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Information Technology Planning Guide](#)**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 and RCW 42.56.365 of the Public Records Act. As such, distribution of this record is limited.**

# State of Washington

**Key Control (Automated Software Calculation - Valuation)** - The external OMAC online portal automatically calculates weekly benefit payment amounts via the Benefit Calculator Tool.

## **STEP 1: Understand Automated Key Control**

After a worker files a Paid Family and Medical Leave (PFML) claim, the external OMAC Portal then automatically calculates payments via the Benefit Calculator Tool. This tool relies on any manual information input by ESD adjudicators during the initial application review, as well as cross-matched data from employer-submitted quarterly wage reports, showing hours worked and employee salary information.

The weekly benefit amount is calculated based on a worker's average weekly wage and the amount actually paid is then prorated based on a comparison of actual to average work week hours. See further understanding of the automated control documented above in the "Controls - OMAC Portal & Dynamics" step, under the section header 'Calculating Benefits'.

## **STEP 2: Confirm and Test Automated Key Control**

### Automated Key Control Confirmation

We confirmed the automated key control via a live walkthrough demonstration with Jeannette Ritchie (Leave and Care Transformation Team Product Manager) and Eric Ayres (Leave and Care Service Delivery Manager), on 6/13/2024, as follows:

We observed as Jeannette navigated to 'Service Cases' and entered case number FJS2YSKM0X-1, which pulled up a 'Benefits Claim - Portal' page. We note that relevant case information was as follows:

- The application was submitted by Janice Marie C Palacios (the claimant) on 6/3/2024.

- Leave start date requested was 5/25/2024 and leave end date requested was 6/10/2024.

- The effective start date and claim year start date was 5/19/2024 and the effective end date was 6/15/2024.

- The qualifying period start date was 1/1/2023.

- There were 2 employers automatically identified by the Portal (due to cross-match with employer quarterly wage reporting): Inifinity Global Distribution LLC and Barmor Temporaries, Inc.

- Current employment status is hourly, or part-time salaried, employee.

- There were no other employers manually added by the claimant.

We note that the Portal's Weekly Benefit Calculator Tool calculated the typical work week hours as 32 and the weekly benefit amount as \$744.

### *Auditor Re-Calculation of Typical Work Week Hours*

As described above in the "Controls - OMAC Portal & Dynamics" step, we found that for non-salaried workers, typical work week hours are calculated as the sum of all hours reported during the qualifying period, divided by 52, rounded down to the nearest hour. The qualifying period is the first four of the last five completed calendar quarters starting from the day the employee intends to take leave.

## State of Washington

The claimant in case number FJS2YSKM0X-1 intended to take leave beginning 5/25/2024. The last five completed calendar quarters were CY23 Qtr 1-4, and CY24 Qtr 1; the first four of which included CY23 Qtr 1-4. During CY23 Qtr 1-4, the claimant worked a total of 1,668 hours, according to previously submitted employer wage reports.

$1,668 / 52 = 32.0769$ , which rounds down to 32. We find that 32 typical work week hours matches the Portal's calculation without exception. **No issues noted.**

### *Auditor Re-Calculation of Weekly Benefit Amount*

As described above in the "Controls - OMAC Portal & Dynamics" step, we found that the weekly benefit amount is calculated as follows. Per ESD's website (see: [esd.wa.gov](https://esd.wa.gov)), for PFML claims filed on or after 1/1/2024, the State's average annual wage was considered to be \$84,167.

A worker's average weekly wage: total reported wages in the claimant's two highest-paid quarters during the qualifying period is divided by 26, then rounded down to the nearest multiple of one dollar.

The weekly benefit amount:

If the worker's average weekly wage is less than or equal to 50% of the State's average weekly wage, then the weekly benefit amount will be 90% of the worker's average weekly wage.

If the worker's average weekly wage is greater than 50% of the State's average weekly wage, then the benefit amount is as follows:

90% of 1/2 of the State's average weekly wage, plus:

50% of the difference between 1/2 of the State's average weekly wage and the worker's average weekly wage.

### Worker's Average Weekly Wage:

We note that the claimant's wages during their two highest-paid quarters during the qualifying period was \$21,875.07.

$\$21,875.07 / 26 = \$841.3488$ , which rounds down to \$841.

### State's Average Weekly Wage:

$\$84,167 / 52 = \$1,618.5961$ , which rounds down to \$1,618 (the State's average weekly wage amount)

$\$1,618 * 50\% = \$809$  (50% of the State's average weekly wage amount)

As the claimant's average weekly wage was greater than 50% of the State's average weekly wage, we re-calculated the benefit amount as follows:

50% of the State's average weekly wage (calculated above) = \$809

90% of 1/2 of the State's average weekly wage:  $\$809 * 90\% = \$728.1$ , which rounds down to \$728.

Difference between 50% of the State's average weekly wage and the claimant's average weekly wage:  $\$841 - \$809 = \$32$

50% of the above-calculated difference:  $\$32 * 50\% = \$16$

## State of Washington

Add 90% of 1/2 of the State's average weekly wage, and 50% of the difference between State and worker average weekly wage:  $\$728 + \$16 = \$744$ .

We find that a weekly benefit amount of \$744 matches the Portal's calculation without exception. **No issues noted.**

### Automated Key Control Testing

**Not applicable** - we are not planning to rely on automated controls and therefore do not need to test automated controls; control risk will be assessed at 'MAX'.

### **STEP 3: Understand General IT Controls**

We gained an understanding of general IT controls as follows: on 7/9/2024, we met with Bryon Schabell (Quality Supervisor), Bora Kim (Delivery Architect), Jeanette Ritchie (Product Manager), and Ed Heredia (Application Manager).

As documented above in the "Controls - OMAC Portal & Dynamics" step, the State average (weekly and annual) wage amounts are calculated annually by ESD's DATA division, based on a computer-generated report within the unemployment (UI) data warehouse. Annually, these average wage amounts and the updated maximum PFML benefit amount are communicated to ESD via the ESD Product Manager. Such communication includes ADO (Azure Development Operations) order requirements, which specify how these amounts are to be applied within the system.

As of CY24, changes to these amounts are made within the 'Manage Program Rates' tool. This tool is presented in a user-friendly format, displaying current values and proposed changes for the following categories: start date, end date, minimum benefit wage, maximum benefit amount, State average weekly wage, minimum qualifying hours, medical leave weeks, family leave weeks, combined leave weeks, and pregnancy complication weeks. Once proposed changes are entered, they are automatically routed for approval (known as 'Pull Requests'). Prior to CY24, changes to rate amounts were made by manually creating pull requests and manually inserting scripts directly into the system.

In all cases, pull requests require approval within the system before they will post to the production environment (**General IT Control 1**). There are a limited number of individuals within ESD who have system-authorization to approve pull requests (i.e., rate changes) (**General IT Control 2**). Currently, there are three individuals with such authorization. All changes and approvals relating to premium rate information are tracked within ADO and git (a version controlling tool which captures changes in system versions).

Prior to approving changes, reviewers will ensure that testing was performed, ensuring correct functioning of the system calculation. The testing phase is completed in five steps: developer testing in the Development environment, testers testing in the Test environment, integration team testing in the Test 2 environment, performance team testing in the Integration Testing environment, and end-to-end team testing in the Staging environment.

### **STEP 4: Confirm Key General IT Controls**

**Key Control 1 - Changes made to the State Average Weekly Wage and maximum benefit amounts (known as 'pull requests')**

## State of Washington

### **require approval within the system before they will post to the production environment.**

On 7/9/2024, we observed as Bora Kim (Delivery Architect) launched Microsoft SQL Server Management Studio, and navigated to the 'OMAC' database, sub-table 'dbo.BenefitConfiguration', and right clicked to select the option 'Select Top 1000 Rows'. We note that the most recent request was created by user ABillington on 12/12/2023. The request included a start date of 1/1/2024, an end date of 12/31/2024, a maximum weekly benefit amount of \$1,456, and a State average weekly wage amount of \$1,618. We note that this amount and the date ranges agree without exception to Work Order 143703 'Adjust PFML Systems for 2024 maximum WBA amount', which was created by Thomas Jones (ESD Product Manager). The pull request was approved by Rebecca Grady (Data Research Team Manager) on 12/12/2023; the pull request 'Status' is currently marked as 'A' (approved), and the 'Update Process' status reads "Operation.ProgramRateManager.Approved()". As confirmed below, Rebecca Grady is an authorized approver for pull requests. **No issues noted.**

### **Key Control 2 - There are a limited number of individuals within ESD who have system-authorization to approve pull requests (i.e., rate changes).**

On 7/9/2024, we observed as Bora Kim (Delivery Architect) launched Microsoft SQL Server Management Studio, and navigated to the 'OMAC' database, sub-table 'dbo.BenefitConfiguration'. Bora then ran the following SQL query: "select 'from Security Permission' where Target Name = STFSYSOPSAPPR". This query generated a list of three individuals who have system authorization to approve pull requests and the associated dates when they were granted such system authorization. The list included: Alison Eldridge (Production Team Manager, added 2/6/2020), John Mattes (Operations Team Manager, added 2/6/2020), and Rebecca Grady (Data Research Team Manager, added 3/19/2020). All users were granted system authorization by the Development Team. **No issues noted.**

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at '**MAX**'.

### **I.7.PRГ - Paid Family & Medical Leave - Expenses**

*Procedure Step:* Key Control 3 (Manual)

*Prepared By:* JLE, 7/16/2024

*Reviewed By:* RKM, 8/13/2024

Purpose/Conclusion:
---------------------

### **Purpose**

To confirm that Employment Security Department staff perform a monthly reconciliation between AFRS and Microsoft Dynamics (Key Control 3 for

## State of Washington

Microsoft Dynamics), in order to assess control risk.

### **Conclusion**

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

## State of Washington

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*



# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 3 (Valuation, Completeness): ESD Treasury staff perform a monthly reconciliation between AFRS and Dynamics, ensuring that amounts reported between the two systems are accurate and complete.**

The understanding for this system is documented above in the "Controls - OMAC Portal & Dynamics" step.

### **1. Confirmation of Key Manual Control**

We obtained the ESD AFRS to Dynamics reconciliation for the month of March (3/1/2024 - 3/31/2024) from Steve Zawoysky (Treasury Manager) on 6/26/2024. The reconciliation was presented in an Excel Workbook named 'Treasury Recon FM09.FY24', and was prepared by Mary Turpin (former Chief Financial Accountant) on 4/27/2024, for PFML Fund 22F.

As noted above in the *Controls - OMAC Portal & Dynamics* step, we would expect the reconciliation to consider data from both Dynamics (AX) and Webi. We noted that the workbook contained tabs for Webi report data and additional tabs formatting Webi information into an Excel pivot table (as noted in tabs 'WebI' and 'Webi Pivot'). The workbook also contained tabs for Dynamics (AX) data, as noted in the tabs 'FM08' and 'AX TB'. A 'Comparison' tab then used Excel formulas to pull data from the 'AX TB' and 'Webi Pivot' tabs for a detailed analysis between AFRS and Dynamics (AX) data. Sub-totals of amounts reported per the 'Comparison' tab then corresponded without exception to the totals seen on the summary tab 'Blank Recon Template' (which is discussed below).

We note that a summary tab, called 'Blank Recon Template' displayed a summary-level description of balances reported per AFRS, compared to those reported per Dynamics (AX). Balance categories included cash, receivables, revenue, liabilities, and expenses. Total differences which needed to be reconciled, reclassified, or corrected for each balance within Fund 22F were as follows:

Cash - \$(4,289,490.47)

Receivables - \$(579,382.84)

Revenue - \$(1,258,994.38)

## State of Washington

Liabilities - \$(536,515.72)

Expenses - \$6,664,383.41

After reconciling these differences, the Treasury team made various adjustments to the amounts reported for Dynamics, as seen on the 'Comparison' tab. After such adjustments, remaining differences (which represent timing differences, as well as unknown variances) were as follows:

Cash - Dynamics overstated by \$568,185

Receivables - Dynamics overstated by \$577,704

Revenue - Dynamics understated by \$16

Liabilities - Dynamics overstated by \$14,411

Expenses - Dynamics overstated by \$4,876

As none of the remaining differences are above the floor, we will not create an audit issue. Steve Zawoysky (Treasury Manager) stated that the unknown variances will continue to be investigated as part of the year-end reconciliation process. We confirmed that ESD Treasury staff perform a monthly reconciliation between AFRS and Dynamics for accuracy and completeness as asserted. **No issues noted.**

### **Noted Weaknesses are as Follows:**

None noted.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at '**MAX**'.

### **I.7.PR.G - Paid Family & Medical Leave - Expenses**

*Procedure Step:* Key Control 4 (Manual)

*Prepared By:* JLE, 10/4/2024

*Reviewed By:* RKM, 10/9/2024

# State of Washington

Purpose/Conclusion:

## **Purpose**

To confirm that the Employment Security Department prepares a year-end journal entry to record an accrual for claims payable, based on actuarial estimates (Key Control 4 for Microsoft Dynamics), in order to assess control risk.

## **Conclusion**

We noted **no** material weaknesses or significant deficiencies in internal controls. **No control weaknesses noted.**

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

## State of Washington

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. *Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. *Controls are not related to a "significant risk" identified in the audit plan.*
- C. *Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all*

## State of Washington

*control testing.*

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 4 (Completeness): At year-end, the Treasury team is responsible for preparing a manual journal entry to record an accrual for claims payable, based on actuarial estimates.**

The understanding for this system is documented above in the "Controls - SAW Portal & Dynamics" step.

### **1. Confirmation of Key Manual Control**

We obtained a copy of the claims payable accrual from Stephanie Eskesen (External Audit Liaison) on 10/3/2024. We reviewed the accrual JV #YEADJ003, noting that it was for \$295,963,207, and that it was appropriately credited to fund 22F, and general ledger account code 5118 (short-term payables, current benefits claims payable). We compared the accrual amount to actuarial workbooks obtained during our 'Rely on Specialist' procedures, noting that the ESD actuary specialist estimated there was an outstanding claims liability of \$295,963,207 as of 6/30/2024. The actuary estimate and claims payable accrual agree without exception. **No issues noted.**

### **Noted Weaknesses are as Follows:**

None noted.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be

## State of Washington

effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at '**MAX**'.

### **I.7.PRG - Paid Family & Medical Leave - Expenses**

*Procedure Step:* Risk Assessment

*Prepared By:* JLE, 8/6/2024

*Reviewed By:* RKM, 8/13/2024

Purpose/Conclusion:

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

#### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

## State of Washington

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be***

## State of Washington

*discussed with the AIC, since they must be reported as findings.*

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Inherent Risk (IR)**

Based on our understanding of the line item, we assessed inherent risk for each relevant assertion and significant class of transactions relating to the Paid Family & Medical Leave Compensation Expenses balance:

**Rights and Obligations - Inherent Risk Assessment - HIGH**

**Valuation - Inherent Risk Assessment - HIGH**



# State of Washington

## **Completeness - Inherent Risk Assessment - HIGH**

### **(2) Control Risk (CR)**

We assessed control risk as follows for each system and relevant assertion:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM)**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**Rights and Obligations - HIGH**

**Valuation - HIGH**

**Completeness - HIGH**

### **(4) Testing Strategy**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

We plan to perform the following tests:

**Rights & Obligations** - We will obtain a population of all PFML claims paid during FY24. Using the sampling spreadsheet from the TeamStore, we will sample claims paid during the fiscal year, determining whether eligibility was properly adjudicated based on: positive applicant identification, qualifying event occurrence, and hours worked (including consideration of whether the correct qualifying period was utilized in the determination).

**Valuation** - We will obtain a population of all PFML claims paid during FY24. Using the sampling spreadsheet from the TeamStore, we will sample claims paid during the fiscal year. Due to the increased risk from manual adjudicator overrides, we will consider stratifying our population into two sample populations (claims which indicate a manual override, and claims which do not). For each testing selection, we will re-calculate the worker's weekly benefit amount paid.

**Completeness** - We will bring in 'Rely on Specialist' procedures from the TeamStore, following all required elements in the associated testing strategy. We will gain an understanding of the source of data used by actuaries to develop the claims payable

## State of Washington

amount, considering whether testing coverage over this data has been adequately addressed in our testing of data relating to the rights and obligations and valuation assertions.

### I.7.PRG - Paid Family & Medical Leave - Expenses

*Procedure Step:* Substantive Testing

*Prepared By:* JLE, 10/9/2024

*Reviewed By:* RKM, 10/10/2024

Purpose/Conclusion:

#### **Purpose**

To determine whether:

- FY24 PFML claimants were eligible for benefits paid (Rights and Obligations)
- FY24 benefit payments were properly accrued during the fiscal year (Completeness)
- FY24 benefits payments were correctly calculated (Valuation)

#### **Conclusion**

We determined that FY24 PFML claimants were eligible for benefits paid, that FY24 benefit payments were properly accrued during the fiscal year, and that FY24 benefit payments were correctly calculated. **No issues noted.**

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

#### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

#### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

## State of Washington

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.7

# State of Washington

## Record of Work Done:

We performed the following substantive tests to meet identified risks and assertions as documented at: [\[Risk Assessment\]](#):

### 1. Rights and Obligations

See testing at: [\[Substantive Testing - Rights & Obligations\]](#).

We obtained two populations from ESD: PFML claims submitted during FY24, and PFML claim benefits paid during FY24. Team IT Audit performed a cross-match between these two populations. Next, we utilized the sampling spreadsheet from the TeamStore to randomly select 39 testing selections from the cross-matched population. To determine whether FY24 claims paid represent valid obligations of ESD, we met with Max Tavaréz (ESD Leave and Care Specialist) on 9/30 and 10/2 via Teams. Max utilized the screenshare function of Teams to demonstrate supporting documentation within the OMAC Portal, LINIX system, and Benefit Calculator Tool. For each testing selection, we viewed identification documentation, medical certification, and employer wage reporting, to determine: whether positive applicant identification was made, whether a qualifying event occurred, whether the correct qualifying period was used in the adjudication determination, and whether the 820 working hours requirement was met by the applicant. We found that all samples were correctly adjudicated and were supported by adequate documentation. **No issues noted.**

### 2. Valuation

See testing at: [\[Substantive Testing - Valuation\]](#).

We obtained a population of PFML claim benefits paid during FY24 from Stephanie Eskesen (ESD External Audit Liaison). We then relied on Team IT Audit to use this data to produce two sub-populations: one of claims which were 'auto-approved' by the Benefit Calculator Tool, and one of claims which were not 'auto-approved', indicating that manual adjustment by adjudicators had taken place. Using the sampling spreadsheet from the TeamStore, Team IT Audit randomly selected 39 samples from each population on our behalf. For these 78 total samples, we requested the following additional information from ESD: claimant wages reported for each quarter of the qualifying period, total hours worked during the qualifying period, whether each claimant was considered to be a salaried or non-salaried worker, and whether the claim week selected for testing was considered to be the claimant's waiting week. For each testing selection, we re-calculated the claimant's base weekly benefit amount, and the weekly benefit amount paid in the given claim week, based on our understanding of RCW 50.04.355, WAC 192-610-051, and WAC 192-610-050 (as documented in the 'Controls' step above). In our recalculation we also tested to ensure the payment didn't exceed the statutory weekly limits. We found no misstatements in our re-calculation of claimant base weekly benefit amounts. For the re-calculation of weekly benefit amounts relating to auto-approved claims, we found an overstatement of \$12, which resulted in projected overstatement of \$576,689. For the re-calculation of weekly benefit amounts paid relating to manually adjusted claims, we found an understatement of \$24, resulting in a projected understatement of \$518,763. Actual and projected misstatements are beneath the floor (both individually and in aggregate). **No issues noted.**

### 3. Completeness

See testing at: [\[Rely on Specialist\]](#).

## State of Washington

We identified a completeness risk that PMFL claims payable benefits were not properly accrued during the fiscal year. After gaining an understanding of the PFML program and controls over claims expense, we found that ESD relies on an internal actuary team to develop a year-end accrual estimate. We brought in 'Rely on Specialist' procedures from the TeamStore, to determine whether we could rely on these actuarial accrual estimates in consideration of our audit work. As part of these procedures, we assessed competency, capability, and objectivity of the actuary specialist. We also gained an understanding of the specialist's procedures and conclusions, and assessed reasonableness of the methods and assumptions used in their work. We additionally gained an understanding of the source data used by actuaries, determining that testing coverage over this data has been adequately addressed in our consideration of population completeness relating to our tests over rights and obligations and valuation assertions. Finally, we assessed reasonableness of the specialist's conclusions, and evaluated whether such conclusions were appropriately reflected in the financial statements. We determined that we can rely on ESD actuarial accrual estimates in consideration of our audit work, specifically noting that specialist conclusions are reasonable, and are reflected in the financial statements. **No issues noted.**

### I.7.PRГ - Paid Family & Medical Leave - Expenses

*Procedure Step:* Rely on Specialist

*Prepared By:* JLE, 10/4/2024

*Reviewed By:* RKM, 10/9/2024

#### Purpose/Conclusion.

##### **Purpose**

To determine if we can rely on the work of the Employment Security Department's Managing Actuary to provide audit evidence for the fiscal year 2024 Paid Family and Medical Leave claims payable estimate.

##### **Conclusion**

We determined that we **can** rely on the work of the specialist. **No issues noted.**

#### Testing Strategy.

To determine whether the audit can rely on the work of the outside specialist and whether the specialist's work supports the financial statements, the following procedures are **required** to be performed:

Auditor should check with their supervisor whenever they determine that the use of a specialist may be necessary.

## State of Washington

*A specialist is an individual or organization possessing expertise in a field other than accounting or auditing (for example, information technology specialists, engineers and actuaries). Specialists may be contracted or employed by entity management to assist them in performing their responsibilities (management's specialist) or contracted or employed by our Office (auditor's specialist).*

*This step does not need to be completed when consulting with attorney general assistants, LGS, TAS, LISA, STAT, DSI or "Subject Matter Experts" designated on the intranet. Contact TAS for assistance if needed to determine whether someone would be considered a specialist or not.*

Assess the specialist's competence, capability and objectivity as it relates to the work that we intend to rely on for the audit.

*Competence refers to the specialist's relevant qualifications and experience. In assessing competence, auditors should consider:*

*The education, professional certifications or licenses of the specialist in his or her field, as appropriate.*

*The reputation and standing of the specialist.*

*The specialist's experience in the type of work under consideration.*

*Our Office's experience in using the specialist's work, if applicable.*

*Capability refers to effect of any access, resource or other limitations on the specialist's work. In assessing capability, auditors should consider:*

*Timing of the specialists work*

*Any significant limitations on the specialist's access to needed information or people*

*Any significant limitations on the time the specialist was able to devote to the work*

*Our Office's experience in using the specialist's work, if applicable.*

*Objectivity refers to the possible effects of any bias, conflicts of interest or undue influence on the specialist's judgment. If the specialist's objectivity is impaired, the auditor may not rely on the work of the specialist. In assessing objectivity, auditors should consider:*

*Any pressures or incentives on either specialists or management to misstate*

*Threats to objectivity of the specialist (including self-interest, advocacy, familiarity, self-review or intimidation threats) and any safeguards in place (segregation of duties, lines of reporting, professional standards, formality and consistency of methods and assumptions, retrospective reviews, etc)*

## State of Washington

*Our Office's experience in using the specialist's work, if applicable.*

*Auditors should contact TAS if the auditor has any concerns with assessing the competence, capabilities or objectivity of specialists.*

Obtain an understanding of the work and conclusions of the specialist. This understanding should include the following elements:

- Objectives and scope of the specialist's work
- Intended use of the specialist's work to support the audit objective
- Specialist procedures and conclusions
- Assumptions and methods used by the specialist

*The objectives and scope of the specialists work and intended use of the specialist's work to support our audit objective should have already been included in the audit plan or else will need to be documented as a change to the audit plan.*

Evaluate the work and conclusions of the specialist. This evaluation should include the following elements as applicable:

Relevance and reasonableness of the specialist's methods and assumptions

*The appropriateness and reasonableness of methods and assumptions used and their application are the responsibility of the specialist. However, if the auditor concludes that the specialist's findings are unreasonable in the circumstances, the auditor should apply alternative procedures, which may include obtaining the opinion of another specialist.*

*Auditors should specifically consider whether methods and assumptions changed from the preceding period and the reasons for such changes, if applicable.*

Appropriate tests of source data provided by the entity to the specialist.

*If any data used by the specialist was provided by the entity, the auditor should consider the risk that incomplete or inaccurate data may materially affect the specialist's conclusions. This risk may be affected by the auditor's assessment of overall COSO elements and control risk for the related system.*

*For example: when relying on work of an actuary for self-insurance liabilities, auditors would normally verify the completeness and accuracy of claims information provided to the actuary against claims information per the pool's system. This can be done by comparing the total claim payments per pool's records to total claims paid shown on the actuary reports (in aggregate or on annual basis) – the figures may not match exactly but should be very close.*

# State of Washington

Relevance and reasonableness of the specialist's conclusions.

Verifying that the specialist's conclusions are reflected in the financial statements

Add an additional representation to the rep letter if the specialist used was employed or contracted by management (rather than SAO). See the List of Additional Representations located in the Auditor Reference Guide here: [Representation Letter Resource.docx](#)

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **SAO Audit Policy [3230](#) - Using the Work of Specialists**

Record of Work Done:

In order to perform the steps below, we met with Eve Sheng (ESD Managing Actuary) on 9/3/2024. Eve performed all actuary procedures relating to the FY24 Paid Family and Medical Leave (PFML) claims payable estimate.

#### **1. Assessment of Competence, Capabilities and Objectivity of Specialist**

We assessed the competence, capabilities, and objectivity of the specialist, specifically considering factors described in the testing strategy, noting the following:

##### Competence

Eve holds a Master of Science from Boston University, and two professional designations: Fellow of the Conference of Consulting Actuaries (FCA), and Member of the American Academy of Actuaries (MAAA). Eve's professional experience spans 17 years and includes work in reserving, pricing, capital modeling, and predictive analytics. As a manager, she has overseen actuarial, data science, and product management processes. Prior to joining ESD, Eve was employed as the Chief Actuary for Liberty Insurance Group's Malaysian operations division. In this role, she evaluated the company's claim liabilities, assessed financial condition, and provided opinions on pricing soundness. She also implemented the first Liberty Specialty Market casualty pricing model. Her position reported to the Board, acted as an ELT member, and was overseen by regulators.

##### Capability

Eve asserted that there were no limitations on her ability to access relevant information, data, or individuals at the Employment Security Department (ESD); however, she noted that for gross wage data, ESD is relying on Statewide employer reporting (via the quarterly wage reporting process). This risk is mitigated by the cross-match that ESD performs during the claim adjudication process (i.e., employee reported wages are compared to employer reported wages for accuracy). The timing of employer wage reporting also creates a small limitation, in that



## State of Washington

wage data is reported a month after the calendar-year quarter ends. To mitigate this limitation, Eve waits to finalize her actuarial estimation amount for claims payable until August (1 month after the end of calendar-year quarter 2). There were no limitations on the time she was able to devote to her work, as development of this actuarial estimation is her primary job responsibility; she holds no other employment outside of ESD.

### Objectivity

During our inquiry, we noted no pressures or incentives placed on Eve or ESD management which would encourage misstatement of the claims payable accrual amount. We note that the ESD actuarial team was initiated in 2022, and that Eve was the first member of this new team. In the future, she will function in a supervisory position and oversee the actuarial work of other staff. However, for the current year, she was tasked with developing the estimation approach and performing the work herself, creating an objectivity threat of self-review.

This threat has been mitigated through collaboration with ESD's finance team. Prior to beginning any work, Eve led internal workshops where she provided detailed information regarding her planned estimation approach. We viewed one of the PowerPoints which she presented, noting that she covered information such as the purpose of a claim reserve, and the implications of different reserving methods. She also demonstrated basic reserving techniques, developed from actuarial standards, to produce paid claim development factors and estimations of incurred but not reported (IBNR) amounts. Eve had to gain the buy-in of ESD upper management and finance specialists in order to proceed with her planned estimation approach, and collaborated with these teams throughout the estimation process. Her final estimation amount was reviewed by these teams, and would not have been relied on if there were disagreements as to the methods used or results of her work.

We noted **no issues** concerning the specialist's competence, capability, or objectivity.

## **2. Understanding of Specialist's Work and Conclusions**

We gained an understanding of the specialist's procedures and conclusions, including the methods and assumptions used, noting the following:

### Specialist Objective and Scope

The primary objective of Eve's work was to develop an accurate estimate of PFML claims payable as of 6/30/2024, for ESD's year-end financial reporting. Scope for this work included historical claims paid data from the inception of the PFML program (which was implemented on 1/1/2020) through present (July 2024 at time of development).

### Specialist's Work in Relation to Audit Objective

The PFML claims expense line item is reported in the Government-Wide Statement of Activities, under the Business-Type Activities opinion unit. This balance represents a new line item selected for testing within the 2024 ACFR audit (i.e., there is no prior audit history for this balance). During initial audit planning, we identified a completeness risk that benefit payments were not properly accrued during the fiscal year. After gaining an understanding of the PFML program and controls over claims expense (i.e., that ESD relies on an internal actuary team to develop a year-end accrual estimate), we refined our risk, considering whether the year-end actuarial estimate for claims payable used reasonable estimation methodology and source data. Eve's work was the primary source used by ESD in developing their year-end claims payable accrual

## State of Washington

amount; as such, her work supports our consideration of the completeness risk for this balance.

### Specialist Methodology

Eve relied on Actuarial Standards of Practice (ASOPs) as a methodology for developing procedures to estimate the claims payable amount. ASOPs provide guidance on the techniques, procedures, and methods that reflect appropriate actuarial practices in the United States. The Actuarial Standards Board establishes and improves such standards of actuarial practice, identifying what the actuary should consider, document, and disclose when performing an actuarial assignment. Current ASOPs indicate that multiple actuarial methods should be used to determine the estimated ultimate losses when completing an actuarial analysis of unpaid claim liabilities. Common methods include: Chain Ladder Methods, Bornhetter-Ferguson Methods, Frequency Severity Methods, and Loss Projection Methods. Eve relied on two methods to perform procedures: the Frequency Severity Method and Chain Ladder Method (CLM).

### *Frequency Severity Method*

The frequency severity method (FSM) is used to determine the expected number of claims an insurer will receive during a time period (frequency), and the average claim's cost (severity). This method looks at past years, in order to determine average costs for future years. First, the actuary gathers historical data on past claims. Then, they analyze collected data to identify trends and patterns for both claim occurrence, and costs. Next, they project future frequency and severity of claims based on those historical trends. Finally, the actuary uses advanced statistical techniques to develop a risk model which incorporates those projected frequencies and severities.

### *Chain Ladder Method*

This method is used to forecast the amount of reserves which must be established in order to cover projected future claims (which are calculated by projecting past claims experience into the future). The method functions by calculating INBR claim estimates, using run-off triangles of paid (historical) claims and incurred (known outstanding) claims. Run-off triangles are two-dimensional matrices which are generated by accumulating claim data over a period of time. This method then relies on the application of a development factor to the known (paid and incurred) losses. Development factors can be based on a company's unique data, on industry data, or a combination of the two. The method can handle data with limited information, making it particularly useful for smaller insurance companies or lines of business with less historical data.

There are seven steps necessary in order to apply the CLM:

- Compile claims data into a development triangle
- Calculate loss development factors (LDFs)\*\*
- Calculate averages of the LDFs
- Select claim development factors
- Select tail factor
- Calculate cumulative chain development factors
- Project ultimate claims

# State of Washington

\*\*LDFs represent the ratio of claim amounts from one valuation date to the next, and are intended to capture growth patterns of claims over time.

## Specialist Assumptions

The significant assumption underlying the Chain Ladder Method is that past claim development patterns will persist in the future (i.e., the development pattern is assumed to be the same for all rows in a loss triangle; no allowance is made to account for change in speed with which claims are settled, or for any other factors which may change the shape of the run-off pattern; each row is assumed to have the same age-to-age development factors).

Accuracy of this assumption depends on the reliability of past loss experience data. Factors such as changes in product offerings, regulatory and legal changes, periods of high severity claims, and changes in the claims settlement process, can impact the validity of these assumptions. Consequently, insurers must continuously evaluate and adjust the model based on actual claim experience to maintain accuracy. If the assumptions built into the model differ from observed claims, insurers may have to make adjustments to the model.

## Specialist Procedures and Conclusions

### *Source Data*

Eve obtains actuarial source data from the ESD Data and Research Team (Leave and Care Division). The Data team used SQL coding to create two tables which run in the ESD1DBOLYLCRD01 server, designed to pull data related to all PFML claims submitted since 1/1/2020. These tables are scripted to run automatically (using a scheduler) on a monthly basis (the 1st of each month at 6am Pacific). The results are then sent to Eve, to ensure relevant and timely information is being utilized in actuarial projections.

The SQL database queries provide 42 columns of information, which are then joined in the two tables. The information contains detailed breakdowns of claim submittal dates, claim adjudication dates, claim benefits paid, leave hours claimed, coding to indicate associated leave type taken, claimant employment status, claimant demographic information, reasons for claim denial, etc.

All columns in the two tables derive directly from columns in the OMAC Portal database and PFML\_DataTeam database, or are simple summations of those columns. The results from these tables are then joined using outer left joins - a command which keeps all rows of the left table, regardless of whether there is a matched key in the right table. A unique identifier assigned to each claim application once it has been submitted, known as ClaimID, was the main key used to join results in these two tables.

### *Procedures*

Eve began by using the FSM to determine averages for each category of claim leave type in her analysis. For example, for family leave claims, Eve determined the number of claims submitted per calendar quarter, and the relevant number of covered employees reported in that same quarter, for the last three years of data from the measurement date (i.e., Q3 of 2021 through Q2 of 2024). This data was used to develop a quarterly incident rate, which was then annualized. Eve translated this into a percent, to show the % of claims ultimately approved out of those submitted

## State of Washington

in a given quarter or year. This approach was used for all categories of claim leave types.

Next, Eve developed run-off triangles using the CLM. There were over 72 triangles developed, examining various factors for each category of claim leave type. For example, in the family leave claim paid amount table, columns were used to represent valuation dates (expressed in months), and rows represent reporting quarters (ex: 20213 = Q3 of 2021). As such, the upper left cell of the table showed the total dollar amount of family leave claim benefits paid, associated with claims submitted during Q3 of 2021, within three months past the end of Q3 of 2021. The cell to the right then showed total claim benefits paid within six months of Q3 of 2021.

The triangles were filled in for all available historical reporting data within the last 3 years, from the date of actuary measurement (Q3 of 2021 through Q2 of 2024), and were updated monthly, based on newly available source data (i.e., most recent data used in the triangles was for claims submitted during Q2 of 2024, paid up to three months after that date).

Next, Eve determined age-to-age factors for each triangle, rounded to the nearest thousandth of a percent. For example, family claims paid (associated with reporting Q3 of 2021), valued as of 3 months, was \$59,584,695. Claims paid for that quarter valued as of 6 months was \$129,535,554, resulting in an age-to-age factor of 2.174 (\$129.5M divided by \$59.5M). These factors were then averaged based on valuation aging. For example, the average 3-6 month aging factor for all historical family claims paid data (Q3 of 2021 through Q2 of 2024) was 2.029. An average was also developed for the most recent 3 and 5 reporting quarters, and the TRIMMEAN Excel function was used to exclude outliers from the 'all quarters' and 'most recent 5 quarters' averages. These averages were calculated for each column (i.e., for each month-to-month valuation date).

Then, Eve developed a 'tail factor', which is used to estimate the additional development that will occur after the eldest maturity in a given run-off triangle. For all triangles, the oldest available data was measured at 36 months after Q3 of 2021. For all triangles, the tail factor used was 1.000 - indicating that no additional activity can be expected for claims 36 months after their submittal date.

Next, Eve used the FSM, tail factor, and age-to-age factors, to calculate an age-to-ultimate factor. These age-to-ultimate factors were used for all tables except the claims paid table. For example, for family leave incurred claims: these age-to-ultimate factors were applied to estimate the ultimate number of claims which would incur weekly benefit payment liabilities, as of a given quarter in which the claims were initially submitted, for all quarters within the past three years. In this particular family leave claims incurred triangle, the 3 month to ultimate factor was 1.084. As of Q2 of 2024, historic data was only available for up to the 3-month valuation period. The total number of claims which were submitted in Q2 of 2024, and which had incurred benefit payment liabilities as of the 3-month valuation period, was 30,539. These total claims were multiplied by the 3 month to ultimate factor of 1.084, to estimate that there would ultimately be 33,107 total claims incurring benefit payment liabilities, which were initially submitted in Q2 of 2024.

Eve utilized these run-off tables and aging factors to estimate for each category of leave: total claims which would incur weekly benefit payment liabilities, total claims which were submitted but which would ultimately be denied, the average number of claim paid weeks per claim, and the

## State of Washington

average weekly benefit amount.

Finally, Eve calculated an estimate of an ultimate claim payable dollar amount (for each category of leave, and for each measured quarter of claims submitted) as follows: estimated total claim weeks \* estimated average weekly benefit amount \* (estimated incurred claims - estimated denied claims). Actual paid claims data was subtracted from the estimate of the ultimate claim payable amount, to arrive at an estimated amount of IBNR claims, for a given reporting quarter. The estimated amount of IBNR claims per quarter was then aggregated for each category of leave, to arrive at a final estimate.

### *Conclusions*

Total liability was summed from IBNR claims, as estimated for each of the past 12 reporting quarters, as follows:

- Q3 2021 (FY22) - \$0
- Q4 2021 (FY22) - \$0
- Q1 2022 (FY22) - \$0
- Q2 2022 (FY22) - \$0
- Q3 2022 (FY23) - \$0
- Q4 2022 (FY23) - \$0
- Q1 2023 (FY23) - \$32,909
- Q2 2023 (FY23) - \$173,597
- Q3 2023 (FY24) - \$2,717,759
- Q4 2023 (FY24) - \$10,031,179
- Q1 2024 (FY24) - \$30,176,058
- Q2 2024 (FY24) - \$252,831,705

For FY24, Eve ultimately estimated there was an outstanding claims payable liability of \$295,963,207.

### **Evaluation of Specialist's Work**

#### Auditor Assessment: Reasonableness of Specialist Methodology and Assumptions

We consider the calculation of INBR claim estimates (via CLM and FSM) to be an appropriate consideration given the nature of PFML reporting. Claimants may apply for leave up to 30 days after a qualifying event occurs. After receiving an 'approved' determination for their application, they then have up to 52 weeks to submit their weekly claims, which can result in a need to backpay claimants at a future date, for past qualifying events (i.e., PFML claims payable liabilities are INBR as of year-end).

We additionally consider significant assumptions underlying the CLM to be reasonable (i.e., the assumption that past claim development patterns will persist in the future). Although accuracy of assumptions can be impacted by changes in product offerings, regulatory changes, process changes, periods of high severity, etc., this risk may be mitigated by the actuary's continuous evaluation and adjustment of the model. Eve is

## State of Washington

employed in her position as Managing Actuary full-time by ESD. Prior to selecting actuary measurement methods, she spent a significant amount of time gaining an understanding of all relevant aspects of the PFML program. Due to her continuous employment, she is kept abreast of any changes affecting the program, which could affect model assumptions. Additionally, she evaluates the model on a monthly basis to determine whether adjustments are needed.

During our review, we inquired whether there have been any significant changes in methods or assumptions used in the prior period. We note that prior to FY23, the ESD Treasury team had been developing a claims payable estimate using various internal methods which did not adhere to any recognized standards or practices. Eve was hired by ESD in 2022, for purposes of establishing credible, more accurate methodologies for the agency; FY23 was the first year in which ESD adopted ASOPs as the basis for their claims payable estimate. There have been no changes in methodology, significant assumptions, or data sources between FY23 and FY24.

We consider the specialist's FY24 methods and assumptions to be relevant and reasonable. **No issues noted.**

### Tests of Source Data

In consideration of our planned testing procedures over the 'Valuation' assertion for the PFML claims expenditure balance, we received a population of all weekly benefit payments made by ESD during FY24, totaling \$1,678,762,707. We compared this total to the FY23 reported balance of \$1,649,030,286, noting that balances are comparable and showing a year-over-year growth pattern, which is consistent with our understanding of the program. We additionally relied on Team IT Audit to perform certain 'reasonableness' procedures over the received data, as documented at: [\[PFML Claims Sample\]](#). Finally, we compared ESD's FY24 claims expenditure data population to balances reported per AFRS, as documented at: [\[Substantive Testing - Valuation\]](#).

We then compared the FY24 claims expenditure data to amounts utilized by Eve within the run-off triangles for 'family' and 'medical' claims paid amounts. Eve's workbook reported \$1,665,767,669 of FY24 claims paid (a difference of \$12,995,038 from the ESD-provided weekly benefit payments population). These differences are due to measurement timing: Eve completed her actuarial estimate for claims IBNR as of 6/30/2024. However, ESD continued to make benefit payments relating to FY24 through 9/15 (i.e., up until the date they booked the year-end accrual). When booking the year-end final accrual amount, the Treasury team then reduces the actuarial estimate by actual claims activity observed in July - September.

Given these differences in measurement timing, we consider the source data used in the actuarial estimate to be complete. **No issues noted.**

### Auditor Assessment: Reasonableness of Specialist Conclusions

Based on our review and assessment of specialist methods, assumptions, source data, and procedures, we have determined that the specialist's FY24 conclusions are reasonable. We specifically evaluated the projected claims payable outcome for each reporting quarter, noting that claims may be paid up to 52 past the date of submittal. We inquired as to the validity of including projected claims payable for claims submitted more than 52 weeks prior to the measurement period (i.e., claims submitted during Q1 of FY23); Eve explained that various scenarios could lead to

## State of Washington

payment streams continuing past 52 weeks of leave start date (e.g., new programs, redetermination processes, checks bouncing and being sent again, payment delay, etc.). We additionally considered the triviality of FY23 Q1 projected claims payable amounts (\$32k), noting that this amount is well beneath the floor for materiality.

We consider the specialist's FY24 conclusions to be relevant and reasonable. **No issues noted.**

### Specialist's Conclusions: Financial Statement Inclusion and Audit Impact

We have documented use of Eve's work to support our audit objective as a change to the audit plan, see: [ ].

As Eve was employed by ESD to complete her work, we have included additional representations to the management representation letter, see: [October 2024 Draft Management Representation Letter].

We verified that Eve's conclusions are reflected in the financial statements through our confirmation of Key Control 4, see: [Key Control 4 (Manual)]. We specifically considered whether the final accrual amount agrees to Eve's actuarial estimate conclusions, noting that the accrual agrees to the actuarial estimate without exception. **No issues noted.**

### I.7.PRГ - Paid Family & Medical Leave - Expenses

*Procedure Step:* PFML Claims Sample

*Prepared By:* PS, 9/17/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion.:

**Purpose:** To select 78 test samples from PFML claims paid in fiscal year 2024.

**Conclusion:** Test samples were provided to audit team.

Testing Strategy.:

Guidance/Criteria.:

# State of Washington

Record of Work Done:

## **Request and Import PFML Claims**

IT Audit emailed Stephanie Eskesen, ESD External Audit Liaison, to request for PFML claims datasets.

An email was sent on August 19th, 2024, to request for the all claims paid in fiscal year 2024. ESD provided the dataset in csv format to us on August 21st, 2024. The files were sent to SAO via the WaTech secure file transfer site (mft.wa.gov). Files were saved to the SAO network drive and imported into SQL database. We have confirmed the record count of the file received with ESD staff. No exception. We have performed procedures at ESD PFML Claims Reasonableness and determined that the data are reasonable.

## **Document Test Objective and Methodology**

Team FA submitted helpdesk 68027 to request for the PFML claims population for fiscal year 2024 so that we can select samples for audit team to determine if claims were calculated correctly.

The following describes the steps taken to meet the test objective:

- Import the fiscal year 2024 PFML claims provided by ESD.

- Create two populations from step 1:

- Population 1: Claims processed by system - IsSystemDecision field = TRUE.

- Population 2: EClaims processed by system - IsSystemDecision field = FALSE.

- Select 39 random transactions from the transactions where IsSystemDecision field = TRUE.

- Select 39 random transactions from the transactions where IsSystemDecision field = FALSE.

As we perform our testing, we will make adjustments to this plan as necessary.

## **Queries**

The queries to complete the testing can be seen at PFML Claims Samples.

## **Reasonableness**

The reasonableness of test results has been performed and documented in the above queries. Based upon our checks, we consider our test results to be complete and reasonable.

## **Results**

Samples were provided to the audit team, through an Excel spreadsheet titled, **!2024\_PFML\_Claims\_Samples.xlsx** (78 records). The file



# State of Washington

provided contain CONFIDENTIAL DATA.

Total PFML claim population	2,605,326 records	\$1,678,762,707.00
IsSystemDecision is FALSE	915,330 records	\$193,935,343.00
IsSystemDecision is TRUE	1,689,996 records	\$1,484,827,364.00

## I.7.PRG - Paid Family & Medical Leave - Expenses

*Procedure Step:* PFML Application and Claims

*Prepared By:* PS, 9/4/2024

*Reviewed By:* JMT, 9/6/2024

Purpose/Conclusion.:

**Purpose:** To identify PFML Applications that have claims in the FY2024 PFML Claims data.

**Conclusion:** We have identify PFML Applications that have claims in FY2024.

Testing Strategy.:

Guidance/Criteria.:

Record of Work Done.:

### **Document Test Objective and Methodology**

Team FA requested for an additional match to the PFML Claims data, see helpdesk 68027. They would like to match a list of PFML applications to the FY2024 PFML claims population to identify applications that have claims.

Step 1: Import the PFML Application list, All\_apps\_submitted\_FY24, provided by Team FA.

# State of Washington

Step 2: Match PFML Application list to PFML Claims data by claim ID.

## **Queries**

The queries to complete the testing can be seen at [PFML\\_ApplicationMatchClaims](#).

## **Reasonableness**

The reasonableness of test results has been performed and documented in the above queries. Based upon our checks, we consider our test results to be complete and reasonable.

## **Results**

Test results were provided to the audit team, through an Excel spreadsheet titled, **!2024\_PFML\_ApplicationsMatchClaims.xlsx**. The results provided contain CONFIDENTIAL DATA.

## **I.8.PRG - Paid Family & Medical Leave - Revenues**

*Procedure Step:* Summary & Conclusion

*Prepared By:* JLE, 10/17/2024

*Reviewed By:* RKM, 11/20/2024

Purpose/Conclusion:

## **Purpose**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

## **Conclusion**

We determined that **no modifications were necessary** to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

# State of Washington

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?

## State of Washington

Were misstatements caused by control deficiencies or circumvention of controls?

If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?

If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.

Did tests identify a different level or type of risk than the planned audit response was designed to address?

If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

# State of Washington

## I.8.PRG - Paid Family & Medical Leave - Revenues

*Procedure Step:* Understanding of Line Item

*Prepared By:* JLE, 6/18/2024

*Reviewed By:* RKM, 8/28/2024

Purpose/Conclusion:

### **Purpose / Conclusion**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

### **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

### **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

(1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).

## State of Washington

(2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.

(3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

### STEP 3: Update Significant Account Matrix

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions**

None.

### **(2) Composition & Change Analysis**

See Line Item Leadsheet at: [[Line Item Lead Sheet](#)].

PFML program revenues represent statutorily-required premiums which are assessed on all Washington State employees and on certain Washington State employers. Such premiums are remitted by employers on behalf of their employees. ESD is responsible for collection and processing all premiums associated with the program. Premiums are calculated at a flat-rate percentage of employee gross wages.

## State of Washington

We analyzed revenue amounts, identifying Revenue Source Code 475 'Paid Family and Medical Leave Premiums' as significant, comprising 100% of total FY23 balance revenues. The AFRS transaction code associated with PFML revenues is 007 'Rcrd Current Rec (Ins)'. Revenues are split between Revenue Sub-Source codes 410 'PFLP' (family leave premiums), 420 'PMLP' (medical leave premiums), and 430 '4109' (voluntary premium plans). Revenue Source Code 475 additionally encompasses related refund activity.

Per our analysis on the 'Balance Detail' tab of the Line Item Leadsheet, we specifically noted the following relating to PFML premiums:

Family leave premium and medical leave premium revenues are equally significant, representing 55% and 45% of total FY23 revenues, respectively.

Revenue from voluntary premium plans is insignificant, representing 0% of FY23 revenues.

Refund activity is also insignificant, representing 2% of FY23 revenues.

We additionally noted that April, July, October, and January represent months of significant PFML premium revenue activity. This is consistent with our understanding of when employer quarterly premium payments are due:

Q1 - due 4/30 (Jan, Feb, Mar)

Q2 - due 7/31 (Apr, May, Jun)

Q3 - due 10/31 (Jul, Aug, Sep)

Q4 - due 1/31 (Oct, Nov, Dec)

During our analysis, we noted a 57% increase between FY22 and FY23 revenues. Per ESD's [FY23 Actuarial Annual Report](#) for PFML (ref: page 8), we found that this change was primarily caused by an increases in the premium rate. During CY21, the rate was 0.4%, which increased to 0.6% in CY22, and increased again to 0.8% in CY23, resulting in the following fiscal year split-rates:

Fiscal Year 2022:

July 2021 - December 2021 = 0.4% rate

January 2022 - June 2022 = 0.6% rate

Fiscal Year 2023:

July 2022 - December 2022 = 0.6% rate

January 2023 - June 2023 = 0.8% rate

*Note: In CY24, the premium rate decreased to 0.74%. FY24 data will have the following associated split rates: July 2023 - December 2023 = 0.8% rate; January 2024 - June 2024 = 0.74% rate.*

Our analysis of the actuarial annual report additionally showed the following:

Covered employees increased approx. 3.1% between Q2 of CY22 and Q2 of CY23.

Taxable (gross) wages increased approx. 9% between Q2 of CY22 and Q2 of CY23.

# State of Washington

**Overall, we identified no unusual or unexpected elements that may indicate unidentified areas of risk for PFML revenues.**

## Additional Background: Program Information

Gross wages subject to PFML premiums are limited by the amount of the federal Social Security cap. The 2024 Social Security cap is \$168,600.

Premium rates are expressed as a total (not by employee v. employer) when being billed. In 2024, the premium rate is .74% of each employee's gross wages (not including tips). The employee's share of the premium is up to 71.43% for FY24, and the employer's share is up to 28.57% for businesses with 50 or more employees.

The PFML program is made up of two claimant categories: medical leave and family leave. Benefits are paid at a rate of up to 90% of a worker's average weekly pay.

Medical leave is provided for an individual's personal health condition (e.g., surgery, pregnancy, mental health, chronic conditions, or inpatient treatment); claimants may receive up to 12 weeks\* of leave per claim year\*\*.

Family leave is provided to assist with a relative's serious health condition, for bonding with newly born/adopted children, and for military family leave relating to deployments; up to 12 weeks\* of leave per claim year\*\*.

*\* If an individual has more than one qualifying event in the same claim year, they may receive up to 16 weeks of combined family/medical leave. If an individual experiences a condition in pregnancy which results in incapacity, they may receive up to 18 weeks of combined family/medical leave.*

*\*\* The claim year begins on the Sunday of the week in which a worker submits an initial application, and expires 52 weeks later.*

## **(3) Updates to Significant Account Matrix**

We updated the relevant accounting systems to include the OMAC Portal, and Microsoft Dynamics.

## **I.8.PR.G - Paid Family & Medical Leave - Revenues**

*Procedure Step:* Controls - OMAC Portal & Dynamics

*Prepared By:* JLE, 7/2/2024

*Reviewed By:* RKM, 8/28/2024

Purpose/Conclusion:
---------------------



# State of Washington

## **Purpose**

To gain an understanding of internal controls within the OMAC Portal and Microsoft Dynamics systems used by ESD; relevant to the valuation and completeness assertions.

## **Conclusion**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy:

## **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.
  - In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.
  - Identify controls systems covering all relevant assertions for all significant classes of transactions.
  - Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.
  - Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.
  - Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

- A brief outline of the transaction flow from beginning to end.

- An expanded description of key controls.

- Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

- Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

- Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

## State of Washington

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

- Who or what initiates the control
- When (or how often) is the control applied
- Who performs the control
- As needed, the experience, knowledge and attitude of the person applying the control
- Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?
- How the key control is documented or evidenced
- If not obvious from the description, how the control prevents or timely detects and corrects misstatements
- Any exceptions or alternative processing to the normal process
- What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

- Initiation:* How are transactions initiated?
- Authorization:* How are transactions and accounting record maintenance authorized?
- Recording:* How are transactions or balances identified and recorded in financial accounting systems?
- Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.
- Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general,

## State of Washington

it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting “each element, in order” because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

Internal controls address the following balance:

Paid Family & Medical Leave Compensation (Premium Revenue)

For the following assertions:

Valuation - There is a risk that premium revenues (rates and gross wages) have not been properly calculated

Completeness - There is a risk that ESD did not identify and follow-up with employers who missed, but were liable for, quarterly wage reporting. There is a risk that the year-end premium revenue accrual amount was not accurately determined based on FY24 premiums due after year-end. There is a risk that balances reported between Microsoft Dynamics and AFRS are incomplete.

### **Gain an Understanding of Internal Controls**

We gained an understanding of internal controls over Paid Family and Medical Leave (PFML) premium revenues as follows:

Meeting with Steve Zawoysky (Leave and Care Division Treasury Manager) and Mary Turpin (Chief Financial Accountant) on 4/25/2024.

Meeting with Nicole Ross (Employer Compliance Manager), Cezanne Levesque (Transformation Manager), John Mattes (Leave and Care Operations Manager), and Rob Rohrer (PFML Customer Service Manager) on 5/20/2024.

Meeting with Rebecca Grady (Leave and Care Research and Data Manager) and Jose Hernandez (Leave and Care Statistical Program Research Specialist) on 5/30/2024.

# State of Washington

Meeting with Imran Shaik (Leave and Care Developer), Bora Kim (Application Developer), Bryon Schabell (Application Quality Assurance Supervisor), and Jeanette Ritchie (Leave and Care Product Manager) on 6/28/2024.

## Premium Rate Calculation

Per [RCW 50A.10.030](#), premium rates assessed for the PFML program are to be determined annually (in October) by the Commissioner, as follows:

- Calculate 140% of the prior fiscal year's expenses (including total amount of benefit claims paid, and the Department's administrative costs)

- Subtract the balance of the PFML insurance account as of September 30th

- Divide the difference by the prior fiscal year's taxable wages (carry to the fourth decimal place, and round up to the nearest 100th of one percent). This determines the total premium rate.

The percentage of premium applied to family leave versus medical leave is then determined as follows:

- Calculate the percentage of paid claims related to family and medical leave benefits separately

- Apply the proportional share of paid claims for each type of leave to the total premium rate

The rate, as calculated above, is subject to two exceptions: first, the total premium rate cannot exceed 1.20%. Second, if the total premium rate exceeds the amount needed to maintain a three-month reserve at the end of the rate collection year, then it must be reduced to the minimum rate necessary to maintain the reserve.

The premium rates are applied based on each individual worker's gross wages. Annually, the maximum amount of individual wages subject to PFML premiums is equal to the maximum amount of wages subject to federal social security tax.

- For family leave premiums - an employer may choose to deduct the full amount of the premium from an employee's wages

- For medical leave premiums - an employer may choose to deduct up to 45% of the premium from an employee's wages

- In all cases, an employer may choose to pay any portion of the employee's share of premiums on their behalf

## *Updating Premium Rates*

There are approximately ten individuals within the Employment Security Department (ESD)'s System Operations team who have the access to edit screens containing premium rate information. Annually, these individuals are tasked with entering the new rates for each category (i.e., employee v. employer premium split, medical leave premium rates, family leave premium rates, and the social security wage cap are all entered separately).

After entering the new rates, these changes are approved by one of three individuals within the Systems Operation leadership team: the Research Manager, Operations Manager, or Deputy Director. The approver verifies the rate change amounts in the 'TEST' environment, comparing prior year rates to current year updated rates. After verifying accuracy, the approver will make these changes live in the production environment. This current rate change process was implemented in December 2023. Prior to this date, the process was handled by ESD's Development team. The process was similar, just performed by a different team - the Development team would insert new rate tables into the database, then publish the

## State of Washington

rate tables and test for correct functioning of calculations, prior to pushing the update into production.

The annual premium rate update process is described in further detail, in the "Key Control 1 (AUTOMATED)" step, under the 'Understand General IT Controls' header.

### Quarterly Wage Reporting and Invoicing

As described in the "Understanding of Line Item" step, employer premiums are due on a quarterly basis. The premium amount is calculated based on gross wage reports, which are submitted directly by employers (or 3rd party administrators) via the Portal. These reports contain additional information such as employee date of birth and total hours worked (including paid time off). As of 10/1/2023, *all* employers must file a report, even if they did not have payroll for the quarter (if they do not have payroll to report, they're expected to file a specific 'no payroll' report). It's important to note that during the invoicing and billing process, there is no difference in how the employer vs. employee's share of premiums is recorded. ESD does not perform procedures to verify how employers are withholding the employee portion of premiums; invoicing and payments are made in total, are billed to the employer, and do not require separate coding.

After a gross wage report is submitted, the Portal automatically creates an invoice for premiums within 24 hours (**Key Control 1 - AUTOMATED - Valuation**). Employers can then make payment using a separate application within the Portal. Payments can be made directly on the Portal via credit card or checks can be mailed to either a U.S. Bank lock box service or to Maple Park headquarters. Mailed checks comprise approximately 1% of total payments received.

### Identifying Missing Reporting

All Washington State employees who work for an employer are subject to pay employee premiums for the PFML program. Corporate officers are considered to be employees for purposes of the program. Self-employed individuals or independent contractors are not considered employees, but may voluntarily opt into the program. Additionally, all Washington State employers with more than 50 employees are subject to pay employer premiums for the PFML program. Exceptions to these requirements include: federal employees, employees of a tribally-owned business on tribal land, self-employed people, independent contractors, and workers covered by an employer's approved voluntary plan.

ESD's Research and Data team is tasked with identifying employers who should be filing quarterly wage reports, but fail to do so. On a quarterly basis, Jose Hernandez (Leave and Care Specialist) performs a cross-match between historical employer wage reporting data per the OMAC Portal and ESD unemployment (UI) data per NGTS, using Department of Revenue (DOR) registered business information, for the purpose of identifying employers liable for PFML premium assessment, but who have failed to file quarterly reports (**Key Control 2 - Completeness**). This process is accomplished as follows:

ESD and DOR have entered into a data-sharing agreement, which allows for DOR State-registered business information to automatically populate within the OMAC Portal. A SQL database within the ESD server houses this information. To begin cross-match procedures, Jose uses SQL coding and 'R' programming language, which tells the system to perform the following steps:

## State of Washington

First, this SQL database is 'grabbed' from the server as a table, displaying a current list of businesses which have an associated unified business identifier (UBI) (UBI's function as individual employer ID numbers - businesses are assigned UBIs when they register to operate within Washington State). The table changes frequently due to new and closing business operations within the State. The report also shows additional data such as business address, legal entity name and contact information. There are approximately 1.5M employer records which populate into the table.

Next, the OMAC Portal is queried for employer wage reporting, by year and quarter. Each row contains reporting history for the total amount of gross wages and number of employees. For cross-matching purposes, the query pulls information for Qtr 1 of 2019 through present day. This data helps ESD identify how many quarters of wage reports are potentially missing for a given employer.

Then, additional table columns are filled in using information from ESD's Next Generation Tax System (NGTS), using a query created by ESD's IT BI team. The NGTS system is where UI reporting takes place and the query identifies employers who have an associated liability start and end date for UI reporting. PFML covers a broader range of individuals than UI, and as such, most businesses reporting UI should also be reporting for PFML. The NGTS data helps ESD identify whether an employer is also liable for PFML premiums.

Ultimately, the SQL and R programming command cross-matches employer quarterly wage reports from the Portal, with UI premium information from NGTS, using DOR UBI records as a 'link' between the two data sets. The programming commands also format this data into a useable format. The end result clearly identifies which employers appear to be missing wage reports for specific quarters, based on UI liability dates. The report also displays a separate list of employers who are missing wage reports, but who do not have an associated UI liability date. These employers require further research to determine whether or not they were truly liable for PFML wage reporting.

After completing his report, Jose then uploads the results in a .csv document to an internal shared drive accessed by the Employer Compliance team, who is responsible for contacting each employer, attempting to bring them into compliance with the program's reporting requirements. As an additional step, adjudicators from the Customer Care team also refer employers to the Employer Compliance team. Adjudicators would make such a referral if a new claim was submitted and ESD discovered there were no employer wages reported on behalf of that employee.

### *No Payroll Reporting*

In place of a quarterly wage report, employers may file a 'no payroll' report, which attests that the employer has no employees for the relevant filing quarter. These reports were implemented in Qtr 3 of 2023 and were developed to help identify the difference between missing wage reports vs. having no wage report to submit. If an employer submits a no payroll report for four consecutive quarters, they have the ability to cease reporting and would no longer be considered an employer in the State.

### **How Transactions are Recorded in AFRS:**

## State of Washington

Employer invoice and payment data is automatically transferred from the OMAC Portal via software integration to Microsoft Dynamics. There are three project codes used by the system when recording transactions: PFLP (family leave premiums), PMLP (medical leave premiums), and 4109 (voluntary payment plans). On a daily basis, Fiscal Analyst 3 (FA3)'s are tasked with uploading Dynamics employer premium and payment data to AFRS using 'Toolbox' software. Prior to releasing the upload, the FA3's work is reviewed by an FA4, Treasury lead, or Treasury supervisor.

On a weekly basis, ESD's System Operations team performs a reconciliation between information captured in the OMAC Portal and data recorded in Dynamics. After completing their reconciliation, the System Operations team generates a spreadsheet summarizing total amounts from both the OMAC Portal and Dynamics, and any variances between the two systems. This spreadsheet is emailed to Steve Zawoysky (Treasury Manager) and other Treasury team supervisors. FA3's on the Treasury team are then responsible for completing any necessary adjusting entries to AFRS.

### AFRS Reconciliation

At the end of each month, Mary Turpin oversees as FA3's perform a reconciliation of information which was reported to AFRS, using 'Toolbox' software. First, they run a monthly summary of the Vendor Payment Journal in Dynamics, showing all monthly activity which was reported to AFRS. Then, they run the 'General Ledger Activity Flexible' WebI report in the Enterprise Reporting system for the same month, showing how AFRS is currently reporting the data for relevant GLs and funds; the coding for PFML premium revenues is Fund 22F, GLs 1312, 1319 and 3210. PFML revenues also hits cash accounts, which are coded as Fund 22F, GLs 1100, 7110, 7120, and 7140. The two amounts are compared for accuracy and completeness (**Key Control 3 - Valuation, Completeness**). Any adjustments needed, such as amounts which are missing a program designation, are completed via the Toolbox software and, as necessary, Form A7-A 'AFRS Journal Voucher'. After reconciling the data and preparing any adjustments, the FA3 will email an approver, requesting that the toolbox reconciliation be reviewed and released. This same process occurs again at year-end, for the entire fiscal years' reporting activity. Mary is responsible for reviewing and approving any year-end reconciliations and adjustments.

At year-end, Mary is also responsible for preparing a manual journal entry to record the accrual of employer premium revenue, based on the 'AFRS Financial Transaction Code' report (**Key Control 4 - Completeness**). This report is run out of the Microsoft Dynamics system at the end of August. For FY24, the report will total premiums due (GL 3210) throughout July and August of 2024. These totals are then used to develop an estimated accrual amount for premium revenue receivable relating to FY24 for reporting purposes. The accrual will be booked for year-end (6/30/2024) and reversed out immediately in the new fiscal year (7/1/2024). July and August are utilized as a basis for the accrual due to the timing of quarterly payments due; the July reporting period covers premiums due for the previous quarter (4/1/2024 - 6/30/2024).

### **Key Controls are as Follows:**

**Key Control 1 (AUTOMATED - Valuation)** - After an employer submits a gross wage report, within 24 hours the external OMAC Portal automatically creates an invoice for premiums due based on the approved premium rate.

**Key Control 2 (Completeness)** - Quarterly, a Leave and Care Specialist performs a cross-match between historical employer wage reporting data per the OMAC Portal, and unemployment data per NGTS, using Department of Revenue registered business information, for the purpose of identifying employers liable for PFML premium assessment, but who have failed to file quarterly reports.

## State of Washington

**Key Control 3 (Valuation, Completeness)** - ESD Treasury staff perform a monthly reconciliation between AFRS and Dynamics, ensuring that amounts reported between the two systems are accurate and complete.

**Key Control 4 (Completeness)** - At year-end the Chief Financial Accountant prepares an accrual JV for PFML premium revenues receivable, based on the 'AFRS Financial Transaction Code' report.

### I.8.PRG - Paid Family & Medical Leave - Revenues

*Procedure Step:* Key Control 1 (AUTOMATED)

*Prepared By:* JLE, 9/24/2024

*Reviewed By:* RKM, 11/8/2024

#### Purpose/Conclusion:

##### **Purpose**

To determine whether the OMAC Portal automatic premium invoice calculation based on approved premium rate (Key Control 1 for the OMAC Portal) was in place and operating effectively, and to consider related general IT controls, in order to assess control risk.

##### **Conclusion**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure the control operated consistently during the audit period; however, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented above in the "Controls - OMAC Portal & Dynamics" step.

#### Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

##### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step.

Auditors should consider the following aspects of the automated control when gaining an understanding:

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?



## State of Washington

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation

- Profile fields (i.e., applicable transaction types)

- Programmed/set formulas and/or values

- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control.

To test the automated control, consider the following procedures:

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

# State of Washington

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses.

Auditors should consider the following aspects of general IT controls when gaining an understanding:

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

## State of Washington

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW.

If general IT controls are tested, consider the following procedures:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

## State of Washington

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**  
**[Information Technology](#) Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

### **STEP 1: Understand Automated Key Control**

After an employer files a quarterly wage report, the OMAC Portal then automatically calculates premium liability and generates an invoice. The calculation is performed based on premium rate information housed in the OMAC Portal, as well as employer size and total gross wages reported per the quarterly wage report.

Employee wages subject to premium are limited to the amount of the federal Social Security cap for any given year (\$168,600 in FY24). Premium

## State of Washington

rates are established annually by the Commissioner for the following categories: family leave, medical leave, employer-level, and employee-level. Premium rate information is then updated annually, in November or December (prior to the start of a new calendar year), based on these Commissioner-established rates, as communicated by the ESD Product Manager (in CY24, this was Thomas Jones).

When generating an invoice, the OMAC Portal bills employers for a total amount due, and does not display the separate rate categories. See further understanding of the automated control documented above in the "Controls - OMAC Portal & Dynamics" step.

### **STEP 2: Confirm and Test Automated Key Control**

#### Automated Key Control Confirmation

We confirmed the automated key control by re-calculating the premium liability amount assessed to ESD Employer ID 100172957 (UBI 603221325). This employer filed a quarterly wage report in Q2 (June) of 2024, reporting \$1,066.32 in gross wages paid subject to premiums. The employer did not participate in any elective coverage programs or voluntary plans. The employer reported 65 employees, and was considered a 'large' employer by ESD.

The employer was assessed \$7.89 in total PFML premiums by the OMAC Portal, with the following coding split:

Employee contribution amount: \$5.63.

Employer contribution amount: \$2.26.

Gross wages subject to premium are limited by social security caps (\$168,600 in CY24). The \$1,066.32 of gross wages is beneath this maximum, as such, the full amount of gross wages are subject to premium. **No issues noted.**

SAO re-calculated the PFML total premium invoice amount, and coding splits, as follows:

Total premium invoice amount:

The CY24 premium rate amount was 0.74%.

\$1,066.32 of gross wages subject to premiums multiplied by 0.0074 = \$7.89. **No issues noted.**

Coding splits:

For CY24, employers with more than 50 employees are responsible for 28.57% of the premium, and employees are responsible for 71.43%.

Employer contribution - \$7.89 multiplied by .2857 = \$2.25. Difference due to rounding. **No issues noted.**

Employee contribution - \$7.89 multiplied by .7143 = \$5.63. **No issues noted.**

SAO re-calculated the premium amount assessed to ESD Employer ID 101172957 without exception, confirming that Automated Key Control 1 was in place and operating effectively during FY24. **No issues noted.**

# State of Washington

## Automated Key Control Testing

**Not applicable** - we are not planning to rely on automated controls and therefore do not need to test automated controls; control risk will be assessed at 'MAX'.

## **STEP 3: Understand General IT Controls**

We gained an understanding of general IT controls as follows: on 6/28/24, we met with Bryon Schabell (Quality Assurance Supervisor), Bora Kim (Delivery Architect), Jeanette Ritchie (Product Manager), and Imran Shaik (Delivery Architect).

Updated premium rate information is communicated to ESD via the ESD Product Manager. Such communication includes the Commissioner-approved rate amounts, as well as ADO (Azure Development Operations) order requirements (such requirements specify how the rates are to be applied within the system).

As of CY24, changes to premium rate amounts are made within the 'Manage Program Rates' tool. This tool is presented in a user-friendly format, displaying current values and proposed changes for the following categories: start date, end date, premium rate, employee medical rate, employee family rate, and premium wage base. The system also displays a list of approved-premiums history. Once proposed changes are entered, they are automatically routed for approval (known as 'Pull Requests'). Prior to CY24, changes to rate amounts were made by manually creating pull requests and manually inserting scripts directly into the system.

In all cases, pull requests require approval within the system before they will post to the production environment (**General IT Control 1**). There are a limited number of individuals within ESD who have system-authorization to approve pull requests (i.e., rate changes) (**General IT Control 2**). Currently, there are five individuals with such authorization. All changes and approvals relating to premium rate information are tracked within ADO and git (a version controlling tool which captures changes in system versions).

Prior to approving changes, reviewers will ensure that testing was performed, ensuring correct functioning of the system calculation. The testing phase is completed in five steps: developer testing in the Development environment, testers testing in the Test environment, integration team testing in the Test2 environment, performance team testing in the Integration Testing environment, and end-to-end team testing in the Staging environment.

## **STEP 4: Confirm Key General IT Controls**

**General IT Control 1 - Changes made to premium rate information (known as 'pull requests') require approval within the system before they will post to the production environment.**

On 6/28/2024, we observed as Bora Kim (Delivery Architect) launched Microsoft SQL Server Management Studio, and navigated to the 'OMAC' database, sub-table 'dbo.PremiumRateRequest', and right clicked to select the option 'Select Top 1000 Rows'. The command displayed one result, which is within expectations given that the current approval request method has only been implemented relating to CY24 rate changes. We note that the request was created by user ABillington on 12/11/2023. The request included a start date of 1/1/2024, an end date of 12/31/2024, a premium rate of .0074, an employee family rate of 0.4805, an employee medicate rate of 0.2338, and a premium wage base of \$168,600. We note

## State of Washington

that these rates and date ranges agree without exception to Work Order 143704 'Adjust PFML Systems for 2024 Premium Rates and Taxable Wages', which was created by Thomas Jones (ESD Product Manager). The pull request was approved by Rebecca Grady (Data Research Team Manager) on 12/11/2023; the pull request 'Status' is currently marked as 'A' (approved), and the 'Update Process' status reads "Operation.ProgramRateManager.Approved()". As confirmed below, Rebecca Grady is an authorized approver for pull requests. **No issues noted.**

### **General IT Control 2 - There are a limited number of individuals within ESD who have system-authorization to approve pull requests (i.e., rate changes).**

On 6/28/2024, we observed as Bora Kim (Delivery Architect) launched Microsoft SQL Server Management Studio, and navigated to the 'OMAC' database, sub-table 'dbo.PremiumRate'. Bora then ran the following SQL query: "select 'from Security Permission' where Target Name = STFSYSOPSAPPR". This query generated a list of five individuals who have system authorization to approve pull requests, and the associated dates when they were granted such system authorization. The list included: Alison Eldridge (Production Team Manager, added 2/6/2020), Baldeep Kang (System Support Specialist, added 7/16/2019), John Mattes (Operations Team Manager, added 2/6/2020), Rebecca Grady (Data Research Team Manager, added 3/19/2020), and Vanessa Lemus (Benefits Specialist, added 1/11/2024). All users were granted system authorization by the Development Team, with the exception of Vanessa Lemus, who was granted authorization by Baldeep Kang. **No issues noted.**

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at '**MAX**'.

### **I.8.PRГ - Paid Family & Medical Leave - Revenues**

*Procedure Step:* Key Control 2 (Manual)

*Prepared By:* JLE, 6/28/2024

*Reviewed By:* RKM, 8/28/2024

Purpose/Conclusion.*
----------------------

### **Purpose**

To confirm that ESD performs a weekly cross-match of OMAC Portal and NGTS unemployment data using Department of Revenue business identifying information, to identify employers who are liable for PFML premium assessment (**Key Control 2 for the OMAC Portal**), in order to assess control risk.

### **Conclusion**

## State of Washington

We confirmed that ESD performs a weekly data cross-match as asserted; however, we found that ESD does not maintain documentation relating to this control activity. **See issue at:** [\[E: ESD PFML Control Weaknesses\]](#).

We **do not** consider this control weakness to represent a significant deficiency or material weakness.

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*



## State of Washington

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

**Key Control 2 (Completeness) - Quarterly, a Leave and Care Specialist performs a cross-match between historical employer wage reporting data per the OMAC Portal, and unemployment data per NGTS, using Department of Revenue registered business information, for the purpose of identifying employers liable for PFML premium assessment, but who have failed to file quarterly reports.**

The understanding for this system is documented above in the "Controls - OMAC Portal & Dynamics" step.

### **1. Confirmation of Key Manual Control**

We confirmed this key control through a live walkthrough demonstration with Jose Hernandez (Leave and Care Specialist) on 6/25/2024, as follows:

First, Jose launched the 'RStudio' program, which is the application used to: access each relevant database, transform data for meaningful analysis, and house saved coding language in in tabs known as 'projects'. Jose accessed the project titled "AllEmployersMissingReports", which brought up approx. 800 rows of coding language. We noted that the code was last updated in April 2024; Jose explained that the code is updated annually during April in order to capture data for the new calendar year (i.e., employer wage reports for CY Qtr 1 (January - March) are due annually in April).

Jose provided the following walkthrough of coding language used and its purpose:

# State of Washington

## Querying the OMAC Portal

Rows 22:28 - RStudio connects to the OMAC Portal database.

Rows 32:35 - Tells the program for which years it should pull employer wage reporting data (currently, language is set to include 2019 - 2024; prior to April, language was set at 2019 - 2023).

Rows 38:51 - SQL code used to query the OMAC Portal database; tells the system to pull employer wage reporting data and create a table in RStudio, by creating objects known as 'data frames'.

Rows 57:67 - RStudio connects to the ESD sub-database housing DOR State-registered business information (the database is located within the OMAC Portal connection).

Rows 71:99 - SQL code used to query for UBI and legal entity name, as well as business contact information (such as address, city, email, etc.)

Rows 103:117 - SQL code used to pull a Wage Transaction table, which identifies employers who submitted reports using a 3rd party administrator, and displays the 3rd party's contact information, such as SAW ID and email.

Rows 142:172 - SQL code used to pull additional employer information about the most recent wage report submitted (when was the submitted, how many employees were reported for, employer size, etc.)

Rows 176:187 - SQL code used to pull information about the number and timing of claims linked to each employer

Rows 191:198 - SQL code used to pull North American Industry Classification Standards (NAICS) for each employer (i.e., industry classification, such as construction, healthcare, etc.)

Rows 203:216 - SQL code used to pull information about employers which have opted out of PFML due to providing an approved voluntary plan

Rows 232:233 - RStudio closes the connection to the OMAC Portal database.

## Querying NGTS

Rows 236:241 - RStudio connects to the NGTS database.

Rows 257:407 - Code created by ESD's BI team, which pulls the following information from NGTS, based on UBI's identified from the OMAC Portal database:

- Employer class

- Unemployment wage reports (excluding tribal and federal employers)

- FEIN (industry number)

- Liability start and end dates (for relevant each relevant reporting year) - this part of the code essentially tells the program to run the entire code for each relevant reporting year (currently coded as 2019 - 2024).

Rows 408:431 - Tells the system to add the information pulled using the code above, to the table created earlier in RStudio (see note on rows 38:51).

Rows 434:435 - RStudio closes the connection to the NGTS database.

Jose demonstrated a few codes and their function, so that we could observe how the individual pieces work. For example, when connected to the

## State of Washington

OMAC Portal, we noted that after running the code in rows 22:28 the 'Connections' display in the upper-right hand of the screen displayed 'Microsoft SQL Server - PFML'. The server contained approx. 15 individual databases; Jose drilled into the OMAC database to show a large amount of sub-databases. These sub-databases are what the program was querying, and their data is displayed as columns within the final report.

Next, Jose provided an overview of the remaining coding language, labeled as 'Steps':

### Step 1 (Rows 440:449)

Jose ran an example of the query for employer wage reporting data (see description of code in rows 32:35 and 38:51). The results generated in the 'Console' display on the bottom of the screen showed 1.4M records, in 3 columns (Employer ID, UBI, and Legal Entity Name). The code in Step 1 (row 444) told RStudio to arrange this data based on CCYYQId; after Jose applied this part of the code, the data then presented 2 columns of data: UBI and CCYYQId. For example, the business with UBI 000000084 displayed three rows of data, showing that they filed employer wage reporting data in: 20192, 20191 and 20193 (i.e., 2019 for Qtrs 1 - 3).

After Jose ran the remainder of the code in Step 1, the employer wage reporting data was transformed from long-format (2 column display) to a wide-format table. Now, UBIs were displayed once per row, and each column represented every reporting quarter from 2019 - (2024 Qtr 1). For quarters where an employer filed a wage report, a 'Y' was entered. For quarters missing employer wage reports, a red 'NA' was entered. The table showed that there were 302,459 employers which have ever reported to ESD for PFML since 2019.

### Step 2 (Rows 464:588)

Jose explained that this step brings in the corresponding liability dates from the NGTS data, and replaces any 'NA's per the table with a date range for that quarter. Then, the system compares this date to NGTS data (using UBIs as the comparative link) checking to see whether that quarter was 'active' (i.e., within boundaries) for employer unemployment liability. If the result is within boundaries, then the employer is considered liable for missing PFML wage reporting. If there is no associated unemployment liability for that quarter (i.e., outside boundaries), then that quarter is not counted as missing.

### Step 3 (Rows 594:598)

This step creates a separate table for employers which were identified as missing quarters of wage reporting, but for which there was no corresponding NGTS unemployment information. This table represents employers which may be liable for PFML wage reporting; such cases require further follow-up from the Employer Compliance team.

The final piece of code is located in row 755; this step tells the RStudio program to save results in a .csv file in a folder called 'Tables'. We observed as Jose accessed an internal folder on ESD's share drive named 'Jose', he then drilled down to sub-folder 'Employer\_Reporting\_Dashboard', and again to sub-folder 'Tables'. We viewed the .csv file which was saved from the week prior on 6/18/2024 titled "allEmployersMissingWR\_WithLiabilityNGTS\_2024-06-18".

# State of Washington

Jose then demonstrated how he shares his results with the Employer Compliance team. He accessed the internal shared folder named 'HW\_DataReportDrop', and drilled down to the sub-folder 'Employer Compliance Data Requests', and again to sub-folder 'All Employers Missing Wage Reports'. Within this sub-folder, was a copy of the same .csv file "allEmployersMissingWR\_WithLiabilityNGTS\_2024-06-18".

Finally, we observed as Jose clicked the 'Source' button in RStudio (this button runs the entire code) at 10:49AM. At 2:18PM, Jose notified us via email that the R script had finished running, producing a .csv file with 300k+ employer records. We obtained a copy of the final .csv file which was ran on 6/25/2024, noting the following:

- The report was titled "allEmployersMissingWR\_WithLiabilityNGTS\_2024-06-25".

- The report included rows for per unique UBI, totaling 302,808 employers.

- Column headers were as follows: UBI, LegalEntityName, InNGTS, LiabilityStartDate, LiabilityEndDate, totalReportsMissingSince2019WithLiability, QuartersMissingPFMLWithLiability\_2019 (and subsequent headers for 2020-2024), Address, City, StateCode, ZipCode, EmployerEmailAddress, Naics3DigitTitle, LastEmployeeCount, LastEmployerSize, TotalApprovedClaims, EmployerWithActiveVP, VPTYPE, mostRecentSawId, and SAWEmailAddress.

- In the column for 'In NGTS', responses were either "UBI appears in NGTS", or "UBI does not appear in NGTS". For employers appearing in NGTS, there was an associated single date in the 'Liability Start Date' column, from as early as 2001; as well as an associated single date in the 'Liability End Date' column (or, for employers with current NGTS liability dates, "NA" was entered in the 'End Date' column). For employers not appearing in NGTS, liability start and end date columns were both marked as "NA".

- In each column for reports missing by year, the specific missing quarter(s) from that year were identified. For example, employer 'Evergreen Implement, Inc.' showed 15 total missing records since 2019, and in 2019 they only missed wage reporting for Qtr 4. However, in 2020, they missed wage reporting for Qtrs 1-4. (We additionally note that this employer's data does not appear in NGTS, which is why there were a higher number of missing records identified; there were no associated NGTS liability dates to help exclude missing wage reports for which there may have not been a reporting requirement).

We determined that all aspects of the final .csv file matched our expectations. We confirmed that ESD performs a quarterly cross-match of NGTS and Portal data (using DOR registered business identifying information) as expected per our control understanding. **No issues noted.**

## **Noted Weaknesses are as Follows:**

None noted.

## **2. Preliminary Control Risk Assessment**

**LOW** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. We will perform testing below to determine if we can place reliance on the controls.

## **3. Control Risk at 'LOW' - Test Key Manual Control**

In order to support a '**LOW**' control risk assessment, we planned to test **all instances of** the control's application during FY24. For each instance of

## State of Washington

control application, we planned to examine whether the **quarterly** cross-match data query was performed according to our understanding, and whether the results were sent to the Employer Compliance team for further follow-up. Per inquiry with Stephanie Eskesen (Audit Liaison) and Jose Hernandez (Leave and Care Specialist) on 8/12/2024, we found that ESD does not maintain documentation relating to this control activity. **See issue in conclusion above.**

As we are unable to test this key control, control risk will be set at '**MAX**'. See final risk assessment and planned substantive testing strategy below in the "Risk Assessment" step.

### I.8.PRG - Paid Family & Medical Leave - Revenues

*Procedure Step:* Key Control 3 (Manual)

*Prepared By:* JLE, 7/16/2024

*Reviewed By:* RKM, 8/13/2024

Purpose/Conclusion:

#### **Purpose**

To confirm that Employment Security Department staff perform a monthly reconciliation between AFRS and Microsoft Dynamics (Key Control 3 for Microsoft Dynamics), in order to assess control risk.

#### **Conclusion**

We noted **no** material weaknesses or significant deficiencies in internal controls. **No control weaknesses noted.**

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

## State of Washington

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

## State of Washington

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 3 (Valuation, Completeness): ESD Treasury staff perform a monthly reconciliation between AFRS and Dynamics,**



## State of Washington

**ensuring that amounts reported between the two systems are accurate and complete.**

The understanding for this system is documented above in the "Controls - OMAC Portal & Dynamics" step.

### **1. Confirmation of Key Manual Control**

We note that Key Control 3 for PFML premium revenues and Key Control 3 for PFML benefit expenditures (for valuation and completeness assertions relating to the Microsoft Dynamics system), are the same key control. See our documentation of control confirmation at: [[Key Control 3 \(Manual\)](#)]. **No issues noted.**

### **Noted Weaknesses are as Follows:**

None noted.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at '**MAX**'.

## **I.8.PRГ - Paid Family & Medical Leave - Revenues**

*Procedure Step:* Key Control 4 (Manual)

*Prepared By:* JLE, 10/17/2024

*Reviewed By:* RKM, 10/28/2024

Purpose/Conclusion:
---------------------

### **Purpose**

To confirm that the Employment Security Department prepares a year-end journal entry to record an accrual for premium revenues receivable, based on the AFRS Financial Transaction Code Report (Key Control 4 for Microsoft Dynamics), in order to assess control risk.

# State of Washington

## **Conclusion**

We noted **no** material weaknesses or significant deficiencies in internal controls. **No control weaknesses noted.**

Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.*

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or*

## State of Washington

*detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.*

***All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.***

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**Key Control 4 (Completeness): At year-end, the Chief Financial Accountant is responsible for preparing a manual journal entry to record an accrual for premium revenues receivable, based on the 'AFRS Financial Transaction Code' report.**

The understanding for this system is documented above in the "Controls - OMAC Portal & Dynamics" step.

### **1. Confirmation of Key Manual Control**

We obtained a copy of the year-end accrual, as evidenced by screenshots of the OFM Financial Toolbox 'Batch Interface to AFRS' file upload detail. On 8/14/2024, ESD uploaded a total batch amount of \$449,045,133.83, with \$445,962,662.48 representing FY25 premiums billed during July and August (related to FY24 CY Q2 wage activity), and \$3,082,471.35 representing associated refund activity, for a total net premium receivable amount of \$442,880,191.13. We note that under 'Results', Toolbox confirmed that the upload process was completed successfully.

We then obtained a copy of the AFRS Financial Transaction Code report, noting that there were six rows of data. Four of these rows were associated with AFRS transaction type 007, account 3210, totaling \$445,962,662.48. The remaining two rows were associated with AFRS transaction type 007R, account 1312, totaling \$3,082,471.35. The combined total of these six rows was \$449,045,133.83. The net amount of transaction types 007 (premium revenue) and 007R (premium revenue refunds) was \$442,880,191.13.

We confirmed that all amounts reported per the AFRS Financial Transaction Code report agree without exception to the OFM Financial Toolbox upload, and FY24 premium revenue receivable accrual. **No issues noted.**

### **Noted Weaknesses are as Follows:**

None noted.

### **2. Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be

# State of Washington

effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test Key Manual Control**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at '**MAX**'.

### **I.8.PR.G - Paid Family & Medical Leave - Revenues**

*Procedure Step:* Risk Assessment

*Prepared By:* JLE, 8/6/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion:

#### **Purpose / Conclusion**

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

#### **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

##### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

## State of Washington

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

### *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be*

## State of Washington

*prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

### **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

### **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria.:

Record of Work Done.:

#### **(1) Inherent Risk (IR)**

Based on our understanding of the line item, we assessed inherent risk for each relevant assertion and significant class of transactions relating to the Paid Family & Medical Leave Compensation Premium Revenue balance:

**Valuation - Inherent Risk Assessment - MODERATE**

# State of Washington

## **Completeness - Inherent Risk Assessment - MODERATE**

### **(2) Control Risk (CR)**

We assessed control risk as follows for each system and relevant assertion:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **(3) Risk of Material Misstatement (RMM)**

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

**Valuation - MODERATE**  
**Completeness - MODERATE**

### **(4) Testing Strategy**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

We plan to perform the following tests:

**1. Valuation** - We will gain an understanding of the premium rate calculation process, including how each calculation input was determined; verifying that the process agrees to our understanding of [RCW 50A.10.030](#) and determining reasonableness of underlying data used in the FY24 calculation. We will obtain specific amounts used by ESD as rate calculation inputs for FY24, re-calculating the FY24 premium rate amounts. Using the sampling spreadsheet from the TeamStore, we will sample and re-calculate premium revenues invoiced during FY24.

**2. Completeness** - To consider completeness of premium revenues invoiced during FY24, we will use Next Generation Tax System (NGTS) data to select a sample of employers who were liable for unemployment premiums during FY24. We will test to ensure that these employers filed PFML quarterly wage reports during the associated period of liability, or, that the ESD Employer Compliance team appropriately attempted to contact the employer regarding their liability. To consider completeness of the year-end premium accrual, we will obtain a copy of the 'AFRS Financial Transaction Code' report for FY24 (which totals Qtr 2 premiums due in July and August of 2024). We will compare totals from this report, to total premium revenue accrued for FY24, determining reasonableness of the total accrual



## State of Washington

amount. We will also obtain a transactional level detail of the data contained within the 'AFRS Financial Transaction Code' report. Using the sampling spreadsheet from the TeamStore, we will sample premiums due after year-end, testing to ensure that accrued premium amounts appropriately relate to premiums during FY24. To consider completeness of the balances reported between Dyamics and AFRS, we will substantiate our population of total premium revenues invoiced during FY24 (population to be obtained as part of our Valuation testing procedures).

### I.8.PRG - Paid Family & Medical Leave - Revenues

*Procedure Step:* Substantive Testing

*Prepared By:* JLE, 10/17/2024

*Reviewed By:* RKM, 10/28/2024

Purpose/Conclusion.:

#### **Purpose**

To determine whether:

All FY24 PFML premiums occurring during the period were reported (Completeness)

FY24 premium rates and revenues were properly calculated (Valuation)

#### **Conclusion**

We determined that all FY24 PFML premiums relating to the period were reported, and that FY24 premium rates and revenues were properly calculated. **No issues noted.**

Testing Strategy.:

Guidance/Criteria.:

Record of Work Done.:

We performed the following substantive tests to meet identified risks and assertions as documented at: [\[Risk Assessment\]](#):

# State of Washington

## 1. Valuation

### Premium Rates

See testing at [\[FY24 Premium Rate Calculation Processes - Valuation\]](#) and [\[FY24 Substantive Testing - Valuation\]](#).

We gained an understanding of the PFML premium rate setting process, specifically considering whether ESD processes agree to RCW 50A.10.030. We then obtained premium rate calculation workbooks and data inputs from ESD, in order to re-calculate the FY24 PFML premium rates, specifically considering reasonableness of source data used by ESD in the calculation. **No issues noted.**

### Premium Revenue

See testing at: [\[FY24 Substantive Testing - Valuation\]](#).

ESD provided a dataset of all premium revenue invoiced for the PFML program during FY24. We utilized SQL queries to consider completeness of the dataset provided by ESD as compared to balances reported in AFRS. We found a difference of \$14.5M between systems, which we found to be caused by the timing of when data was pulled for our population, vs. the timing of when data is reported to AFRS. Our audit testing provided 100% balance coverage of the amount reported per the AFRS database. **No issues noted.**

Utilizing stratification methods and the sampling spreadsheet from the TeamStore, we randomly selected 32 samples to test. For each testing selection we re-calculated the premium assessed, based on: the applicable premium rate, the number of employees reported, and the amount of gross wages paid to employees. **No issues noted.**

## 2. Completeness

### Premium Revenues Invoiced (Employer Quarterly Wage Reporting)

See testing at: [\[FY24 Substantive Testing - Completeness\]](#).

We relied on Team IT Audit and utilized the sampling spreadsheet from the TeamStore to obtain a sample of employers who were liable for FY24 unemployment premiums from ESD's Next Generation Tax System (NGTS). We obtained two separate populations and samples: employers which were considered delinquent per NGTS, and those which were not. For each sample selection, Team IT Audit performed a cross-match to PFML premium data from the OMAC Portal system, based on Unified Business Identifier (UBI), in order to determine whether the employer had submitted quarterly wage reports for PFML premiums during FY24. For those employers which had not submitted PFML quarterly wage reports, we met with Nicole Ross (ESD Employer Compliance Manager), to understand ESD's processes for following-up with each employer, and whether they were ultimately determined to be liable for PFML quarterly wage reporting. We found that all employers from our sample either filed PFML quarterly wage reports, or were not liable for PFML reporting. **No issues noted.**

### Year-End Premium Accrual

See testing at: [\[FY24 Substantive Testing - Completeness\]](#).

We obtained copies of the AFRS Transaction Report and associated transactional level detail (represented by LCD Customer Invoice Journal Reports). Utilizing the sampling spreadsheet from the TeamStore, we haphazardly selected 30 samples to test. For each testing selection, we

## State of Washington

received screenshots of employer 'Wage Submission History' from the OMAC Portal, and determined whether: the relevant wage reporting period was within FY24, the recorded premium amount per the Portal agrees to the accrued premium revenue amount, and whether the employer wage submission date fell on, or before, the invoice date. We determined that premium revenues accrued at year-end were appropriately related to FY24 activity, noting no exceptions within our testing. **No issues noted.**

### I.8.PRQ - Paid Family & Medical Leave - Revenues

*Procedure Step:* PFML Premium Population

*Prepared By:* PS, 9/30/2024

*Reviewed By:* JMT, 10/1/2024

Purpose/Conclusion.:

**Purpose:** To select test samples from PFML premium in fiscal year 2024.

**Conclusion:** Test samples were provided to audit team.

Testing Strategy.:

Guidance/Criteria.:

Record of Work Done.:

### **Request and Import PFML Claims**

IT Audit emailed Stephanie Eskesen, ESD External Audit Liaison, to request for PFML Premium datasets.

An email was sent on August 19th, 2024, to request for the all PFML premium billed in fiscal year 2024. ESD provided the dataset in csv format to us on August 27th 2024. The files were sent to SAO via the WaTech secure file transfer site (mft.wa.gov). Files were saved to the SAO network drive and imported into SQL database. We have confirmed the record count of the file received with ESD staff. No exception.

# State of Washington

The audit team has added an additional test for this data. They would like to match PFML Premium to NGTS delinquent and non-delinquent employers. To perform this test we will need the UBI and FEIN numbers for the employers in the PFML Premium dataset. ESD staff added the two additional fields to the PFML Premium dataset and sent it to us on September 11th, 2024. Files were saved to the SAO network drive and imported into SQL database. We have confirmed the record count of the file received with ESD staff. No exception.

## **Document Test Objective and Methodology**

Team FA submitted helpdesk 68026 to request for the fiscal year 2024 PFML premium dataset.

The following describes the steps taken to meet the test objective:

- Import the fiscal year 2024 PFML premium provided by ESD.
- Determine if the dataset provided is reasonable.
- Select 31 random transactions for audit team. This was completed but the average premium amount of the samples did not meet expectation. This sample was not use for testing.
- Stratified the PFML premium population for audit team.
- Select sample size per instruction from audit team.

As we perform our testing, we will make adjustments to this plan as necessary.

## **Queries**

The queries to complete the testing can be seen at [PFML Premium Samples](#). After selecting the samples, we realized that the average premium amount of the samples did not meet expectation. It was about 27% of the average premium amount of the test population.

To address this, we have prepared a stratified summary of the total population for the audit team at [!2024\\_PFMLPremiumPopulation&Samples](#). Using this, the audit team will select sample size for testing.

## **Reasonableness**

The reasonableness of test results has been performed and documented in the above queries. Based upon our checks, we consider our test results to be complete and reasonable.

## **Results**

Samples were provided to the audit team, through an Excel spreadsheet titled, **!2024\_PFMLPremiumPopulation&Samples.xlsx**. The file provided does not contain CONFIDENTIAL DATA.

# State of Washington

A table of Stratified Population  
32 samples per request from audit team as:

- Strata 1 (transactions ranging from \$25.01 to \$4,000): 6 samples
- Strata 2 (transactions ranging from \$4,000.01 to \$50,000): 9 samples
- Strata 3 (transactions ranging from \$50,000.01 to \$800,000): 10 samples
- Strata 4 (transactions \$800,000.01 or greater): 7 samples

## I.8.PRG - Paid Family & Medical Leave - Revenues

*Procedure Step:* PFML Premium CAATS  
*Prepared By:* PS, 9/11/2024  
*Reviewed By:* JMT, 9/12/2024

Purpose/Conclusion.:

**Purpose:** To determine if a random sample selection of delinquent employers and non-delinquent employers was billed for PFML premiums.

**Conclusion:** We have identified employers who were billed and those who were not billed PFML premiums. Results provided to audit team.

Testing Strategy.:

Guidance/Criteria.:

Record of Work Done.:

# State of Washington

## **Request and Import PFML Claims**

IT Audit team had requested for PFML Premium dataset from ESD and imported the dataset into SQL. Details of the request and import is documented at [PFML Premium Population](#).

## **Document Test Objective and Methodology**

Team FA, Jessica Elsner, has provided a list of delinquent and non-delinquent employers ([UF Premiums and Assessments Sample Selections](#)) and requested that we determine if these employers had PFML premiums billed. This request will be added to helpdesk 68026.

The following describes the steps taken to meet the test objective:

Import the delinquent and non-delinquent employers lists provided by audit team.

Add employers UBI and FEIN to the delinquent and non-delinquent list.

Match delinquent and non-delinquent employers lists to PFML Premium by UBI (if UBI is unavailable, match by FEIN) to determine if they were billed for PFML Premium.

As we perform our testing, we will make adjustments to this plan as necessary.

## **Queries**

The queries to complete the testing can be seen at [PFMLPremiumEmployersMatch](#).

## **Reasonableness**

The reasonableness of test results has been performed and documented in the above queries. Based upon our checks, we consider our test results to be complete and reasonable.

## **Results**

Results were provided to the audit team, through an Excel spreadsheet titled, **!2024\_PFML\_Premium\_Employers.xlsx**. The file provided contain CONFIDENTIAL DATA.

Delinquent employers and the total premium amount billed - 57 records

Non-delinquent employers and the total premium amount billed - 57 records.

## **J.1.PRG - Community and Technical Colleges**

# State of Washington

*Procedure Step:* Summary & Conclusion  
*Prepared By:* DRR, 11/19/2024  
*Reviewed By:* RKM, 11/20/2024

## Purpose/Conclusion:

### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk, or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

## Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:

# State of Washington

## Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria.*
---------------------



# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

Record of Work Done.:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

**(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

**(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

### **J.1.PRG - Community and Technical Colleges**

*Procedure Step:* Understanding of Line Item

*Prepared By:* DRR, 5/21/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion.:

**Purpose / Conclusion:**

To gain an understanding of the line item and confirm the scope of testing as documented in the Significant Account Matrix.

Testing Strategy.:

Auditors are **required** to perform the following procedures for each line item:

# State of Washington

## **STEP 1: Prior Audit Exceptions**

Document any exceptions noted during the prior audit. Follow-up to determine how the agency has responded to or corrected the issue, unless this work is anticipated as part of the testing strategy.

## **STEP 2: Analyze Composition and Changes of Line Item**

Include link to the line item leadsheet. This will be completed at the end of the audit. Leadsheet analysis should be documented in this spreadsheet.

Inquire with agency staff about the activities and transactions that make up the balance and any changes to those activities or transactions in relation to the prior year.

Determine relevant classes of transactions or account balances within the line item to analyze (such as agencies, funds, programs, departments, accounts, and/or objects), and use AFRS to create trends of those elements. This step should not include any specific dollar amounts associate with the line item.

Evaluate trends to identify:

- (1) What classes of transactions or account balances are primary to the identified risk. Auditors should specifically consider what elements are primary to the line item (comprising a large percentage of the line item), and which elements the identified risk would apply to, and which elements might be most susceptible to the identified risk (having a high risk of non-trivial misstatement for a relevant assertion, considering likelihood and impact of potential for misstatement).
- (2) What changes are primary to the identified risk, if applicable. Auditors should specifically consider whether the overall change to the line item from the prior year was significant, what elements were the primary drivers of overall change, whether any elements changed significantly from the prior year, and which changes (if any) might relate to the identified risk.
- (3) Any unusual or unexpected elements, amounts, or changes that may indicate a risk, whether the one identified in planning or a new one that may need to be considered for a change to the plan.

**Consider** other procedures to gain an understanding of the line item, such as review of key policy documents, review of program information or reports, inquiry of staff, budget information, or other analytical procedures.

## **STEP 3: Update Significant Account Matrix**

Based on your understanding of the line item, update the Significant Account Matrix with final conclusions on the agencies covered, account description, significant accounting systems, and risk (what could go wrong and relevant assertions). The account description should reflect the significant transaction streams or account balances relevant to the risk.

*The description of agencies, significant accounting systems, and what could go wrong in the Significant Account Matrix constitute the overall scope of substantive testing.*

*A transaction stream is significant based on the potential for misstatement. This is often due in part to its size (ie: comprising a large*

## State of Washington

*percentage of the total line item), but is ultimately a judgment about the susceptibility to the identified risk (for example, when the risk is understatement a small or omitted account may hold the most potential for the largest misstatement).*

*Significant accounting system(s) are those that contain key controls over significant classes of transactions included in the line item. Control systems identified in this step must match the Significant Account Matrix and have a separate control understanding documented.*

*Talk with the AIC if you identify any changes to the Significant Account Matrix.*

Guidance/Criteria.:

Record of Work Done.:

### **(1) Prior Audit Exceptions:**

The State Board of Community & Technical Colleges (SBCTC) had prior audit exceptions that were included in the FY23 ACFR Management Letter [[ACFR 2023 Management Letter OFM and SBCTC](#)]. See contents of ML below:

### **State Board for Community and Technical Colleges – Reconciliations and Adjustments**

The State Board for Community and Technical Colleges (SBCTC) advocates for, coordinates and directs Washington's system of 34 public community and technical colleges. One of the SBCTC's responsibilities is to collect and consolidate community and technical college financial data for reporting in the state's general ledger accounting system.

The state produces a series of year-end exception reports designed to identify potential errors in financial reporting. Based on our review of these reports, we found several likely errors that should have been investigated and corrected. The SBCTC did not actively work, investigate, and adjust several of the high-risk balances noted in these reports, including:

Unchanged balance sheet accounts (\$10.6 million) that likely needed adjustment

Negative assets (\$56.0 million) that likely needed adjustment

Negative liabilities (\$9.6 million) that likely needed adjustment

In addition, colleges reported their receipts of federal direct student loans as federal revenue, rather than a reduction in expenditures. This resulted in a \$30.4 million overstatement of federal grants in aid revenue, as well as a corresponding overstatement in expenditures within the special revenue higher education fund. These errors were not corrected in the financial statements.

We recommend the SBCTC:

Actively work with colleges to investigate and adjust exception report balances provided by OFM, when appropriate

## State of Washington

Work with OFM in its reconciliation of direct federal assistance to ensure the proper accounting and recording of federal revenues

As we will develop follow-up testing procedures, we did not follow-up with SBCTC staff regarding their response or correction of this issue.

### **(2) Composition & Change Analysis:**

Line Item Leadsheet: [[Line Item Lead Sheet](#)].

There are **nine** material balances selected for audit that contain activity related to the State Board for Community and Technical Colleges (SBCTC). There are a total of 34 Community & Technical Colleges in Washington state. However, for the purposes of reporting in AFRS there are 30 Colleges as the Spokane, Pierce and Seattle Colleges all get rolled into their respective "parent" College. For example, Pierce College's data will include both the Steilacoom and Puyallup campuses. As such, throughout our work on for "Community & Technical Colleges", we will refer to 30 Colleges. The Colleges' data is uploaded to AFRS under the Board's agency number (699) because in AFRS the data is not broken down by College. AFRS shows SBCTC as a single entity, which includes all of the Community Colleges.

The State Board is responsible for reconciling the community college accounting system (subledgers) for reporting in AFRS under one fund (agency 699). This section is to review the reconciliation of the subledger data to AFRS. We test selected individual colleges for accuracy of information and review the reconciliation of the community and technical college system as a whole for completeness and accuracy.

We selected the following specific account balances for review at SBCTC for FY 2024:

- Cash and Cash Equivalents
- Depreciable Assets (Net of Accumulated Depreciation)
- Charges for Services
- Federal Grants-In-Aid
- Education Expenditures

For the purpose of the state ACFR, all of the reconciliations for FY2024 were performed by Sue Willis, System ctcLink Accounting Manager, and reviewed by Teri Sexton, Agency Accounting Manager. There were no major changes to SBCTC's CEMLI (pronounced Kim-lee) process, but they did make minor changes to update some original coding for efficiency. CEMLI stands for Configuration, Extension, Modification, Localization, and Integration; CEMLI is the in-house developed software program used to upload Peoplesoft data directly into AFRS.

Teri Sexton, Director of Accounting and Business Services, indicated that when changes or updates to the CEMLI process are deemed necessary, SBCTC accounting staff identify the needs and reach out to the SBCTC data services team to update the processes. The changes or updates are then tested in a test environment before being put into production. Staff monitor these changes to be sure that they are working as intended.

We identified that the State Board is in the process of completing a ctcLink Accounting manual (CLAM) to replace the legacy accounting manual or

# State of Washington

FAM. It is posted on their [website](#) for College & SBCTC Staff under accounting and business services. The web page states that:

"The purpose of this manual is, in part, to fulfill the Washington State Board for Community and Technical Colleges' (SBCTC) responsibility under RCW 28B.50.090 (7)(b) to "Establish minimum standards to govern the operation of the community and technical colleges with respect to internal budgeting, accounting, auditing, and financial procedures as necessary to supplement the general requirements prescribed pursuant to Chapter 43.88 RCW."

## **(3) Updates to Significant Account Matrix:**

None.

## **J.1.PRG - Community and Technical Colleges**

*Procedure Step:* Controls - ctcLink System Reconciliation

*Prepared By:* DRR, 5/21/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion.\*

### **Purpose:**

To gain an understanding of internal controls.

### **Conclusion:**

We gained an understanding of internal controls as documented in the record of work done.

Testing Strategy.\*

### **The following procedures are required for all material systems:**

1. List the financial statement balance(s) and relevant assertion(s) addressed by the understanding.
2. Gain an understanding of the internal control process, identify how transactions are recorded in AFRS, identify key controls over relevant assertion(s), and note any control weaknesses.

## State of Washington

In gaining an understanding of controls, consider the overall understanding of State-Level control elements as documented in the "State-Level Controls" step as they relate to this particular system.

Identify controls systems covering all relevant assertions for all significant classes of transactions.

Standards require the auditor to gain an understanding of the significant accounting system(s) that contain key controls over significant classes of transactions included in the line item.

Control systems identified in this step must match the Material Account Matrix and have a separate control understanding documented.

Talk with the ACFR Specialist or AIC if you identify different systems than the ones anticipated in the Material Account Matrix.

For each material system, auditors must document:

A brief outline of the transaction flow from beginning to end.

An expanded description of key controls.

Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.

Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger (AFRS) or financial statements.

Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

The following is information to **consider** when identifying key controls and transaction flow.

"Key controls" refer to the few controls that together provide reasonable assurance that material misstatements will be prevented or detected and corrected. This is contrasted with ancillary or supporting controls, which – although helpful and recommended – would provide less than reasonable assurance by themselves.

The focus of the write-up is on the key controls. Key controls should be specifically identified (as "key controls") in the write-up. This can be done in whatever way the auditor prefers, so long as it is obvious. Details that the auditor should document regarding key controls may include:

Who or what initiates the control

When (or how often) is the control applied

Who performs the control

As needed, the experience, knowledge and attitude of the person applying the control

## State of Washington

Detailed description of the control process or activity. For example, if the control is a review: what exactly is reviewed, what is the reviewer looking at or for and what are the reviewer's criteria?

How the key control is documented or evidenced

If not obvious from the description, how the control prevents or timely detects and corrects misstatements

Any exceptions or alternative processing to the normal process

What happens when misstatements or issues are identified by the control

The "transaction flow" refers to the process by which transactions are initiated, authorized, recorded, processed and reported (as applicable). Outlining the transaction flow gives context to key controls, especially how transactions become subject to controls in the first place. If a control inherently ensures that all applicable transactions are included (ex: bank reconciliation where the assertion is existence), the auditor may decide to just start the write-up with the initiation of the control procedure and go from there.

Elements of the transaction flow are defined informally as follows:

*Initiation:* How are transactions initiated?

*Authorization:* How are transactions and accounting record maintenance authorized?

*Recording:* How are transactions or balances identified and recorded in financial accounting systems?

*Processing:* How are the transactions or balances processed after they are recorded (if at all)? Processing may be manual or automated and may occur at a subsidiary system level or at the general ledger level.

*Reporting:* How are records translated into the financial statements? This part of the transaction flow extends the understanding to the actual financial statements that the audit is opining on. Since we already document an understanding of the financial reporting process in general, it is usually enough to simply reference this overall understanding. However, if there are important steps unique to the covered balances, it may be more appropriate to mention them here.

Although transaction flow is a good way to think about understanding and documenting a control system, auditors should not worry too much about documenting "each element, in order" because often elements may be combined, not noticeable, not applicable or occur in a different order.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

## Financial Statement Audits Planning Guide

Record of Work Done:

Internal controls in the ctcLink System Reconciliation process address the following balance(s):

### **1. Higher Education - Special Revenue:**

- AC - Cash and Cash Equivalents (Local Portion)
- CG - Federal Grants-In-Aid
- CH - Charges for Services
- FS - Education

### **2. Governmental Activities:**

- 2C - Depreciable Assets (Net of Accumulated Depreciation)
- 2C - Education - Higher Education - Charges for Services
- 3C - Education - Higher Education - Operating Grants & Contributions
- G3 - Education - Higher Education - Expenses

### **3. Higher Education Student Services Fund:**

- AC - Cash and Cash Equivalents (Local Portion)

For the completeness assertion.

### **Gain an Understanding of Internal Controls**

We met with Sue Willis, ctcLink Accounting Manager, on April 29, 2024 to gain an understanding of internal controls for SBCTC's ctcLink to AFRS reconciliations. For documentation purposes, the controls to ensure that all financial data submitted to the State Board of Community and Technical Colleges (SBCTC) from each college is uploaded from the ctcLink (PeopleSoft) to the Agency Financial Reporting System (AFRS) will be called the "Reconciliation Process". We will perform testing at three colleges to ensure that the data received by the State Board is accurate. The selected colleges are:

- Seattle Colleges [Community & Tech College Testing - Seattle]
- Community Colleges of Spokane [Community & Tech College Testing - Spokane]
- Bellevue College [Community & Tech College Testing - Bellevue]

We will gain an understanding of the controls over the reconciliation process to ensure that financial data uploaded from ctcLink is complete, properly valued and recorded into AFRS correctly. We will focus our discussion on the following systems:



## State of Washington

**ctcLink (PeopleSoft)** - The single, centralized system of online functions to give students, faculty and staff a way to do college business. ctcLink is an Oracle PeopleSoft application and is referred to by either ctcLink or just Peoplesoft. As of July 30, 2022, all 30 colleges and the SBCTC were using ctcLink, the centralized online system that replaced the outdated FMS Legacy system. The conversion to ctcLink was rolled out to the colleges and the SBCTC over the last few years.

**CEMLI** - The software that SBCTC developed to convert ctcLink data into AFRS data. See below for more information.

### **How transactions are recorded in AFRS:**

SBCTC is responsible for tracking and recording the financial data that is submitted by all of the Community & Technical Colleges, through the ctcLink system. There are a total of 30 Community & Technical Colleges in Washington state. The Colleges' data is uploaded to AFRS under the Board's agency number (699) because in AFRS the data is not broken down by College. AFRS shows SBCTC as a single entity, which includes all of the Community Colleges.

On November 19, 2024, we met with Sue Willis, ctcLink Accounting Coordinator, Kelly Diaz, Statewide Accounting Supervisor, and Lori Carambot, Associate Director of Accounting, to gain an understanding of how SBCTC converts some college data from full accrual to modified accrual for reporting in the special revenue funds for the ACFR. Lori explained that the transactions that roll up into the special revenue fund focus on the inflows and outflows of current resources such as current assets and current liabilities. As such, long term liabilities and non-current assets are not reported in these funds. She mentioned that grant and tuition revenue is reviewed at fiscal year end to determine which amounts are unearned and when they will be available for use. SBCTC will back out revenue as needed to record as unearned revenue. The college system does not allow pre-paid expenses and in the special revenue fund, SBCTC will only report expenses that have been incurred. SBCTC ensures that non-applicable expenditures such as depreciation are not included.

We also identified all funds in the Higher Education Special Revenue opinion unit (roll up fund FBG) here [[Special Revenue Classification](#)] and related ACFR queries. We used OFM's [fund reference guide](#), associated RCWs, and OFM's fund classification review in excel worksheet "Rest\_FBG\_Sp\_Rev\_fund\_by\_rev\_source\_Final\_FY2024.xlsx" to determine if OFM is properly reporting these funds as special revenue. To assist in our determination, we obtained definitions for [enterprise funds](#) and [special revenue funds](#) from SAO's website which uses GASB definitions.

### **General Ledger information & AFRS crosswalks:**

We documented the crosswalk and converted the material balance accounts in AFRS to ctcLink ledgers accounts on the Line Item Lead Sheet here: [[Line Item Lead Sheet](#)] - See "ctcLink Mat Bal Accts" tab and "COA Crosswalk" tab.

Each sub object and source of revenue has its own general ledger account in the ctcLink system and these are converted back to AFRS GL accounts 6510 and 3210 monthly and at year end during the college data consolidation and upload to AFRS process performed by Sue Willis. ctcLink general ledger accounts are 7 digit numerical accounts grouped by the leading digit as assets, liabilities, expense, revenue, or equity. The system also has budgetary only accounts that correspond to these groupings.

Sub Object or Expense accounts in ctcLink generally begin with "5".

## State of Washington

Source of Revenue or revenue accounts generally begin with "4"

The exception is that object "S" (interagency or inter college reimbursements) which are reported/uploaded to AFRS as GL 6510 expenses were grouped in the revenue category in ctcLink.

Each College's monthly General Ledger data is updated by the manual closing of "submodules" by College finance staff about 5 days before each month end and a few days after year end, June 30, of each fiscal year. Transactions within the submodules post to various general ledger accounts such as student financial tuition and fee revenue, accounts payable expense transactions, payroll expenses, accounts receivable and billing updates, grant revenue and expenditures, and Treasury transactions for cash and cash equivalents. The journals created by the submodules are reviewed at each college by staff responsible, and then posted to the GL.

The submodules are listed below:

<b>Sub Module Code</b>	<b>Sub Module Title</b>
AM	Asset Management
AP	Accounts Payable
AR	Accounts Receivable
BI	Billing
CA	Contracts/Grants
EX	Expenses
GL	General Ledger
HR/HCM	HR Payroll
SF	Student Financials
TR	Treasury

The College General Ledger accounts are also updated with journal entries throughout the month and during the adjusting period 13, typically July 1 through the first week of August each year. No adjusting entries are processed through the sub modules, so any accruals or asset adjustments are done through journal entries to the general ledger during period 13. It is also important to note that not all Colleges are using all of the submodules within ctcLink. Some Colleges are not using the Asset Management (AM) Module and instead update Capital Asset general ledgers using journal entries and track college assets using the DirectLine system as they did during use of the Legacy FMS system. Other Colleges might not utilize the Travel and Expenses (EX) or the PCard system within the Accounts Payable sub module, and instead continue to use travel voucher paper forms and manual entries into to the Accounts Payable system. The reason for this is the College's continue to face challenges coordinating College wide staff training and staff turn-over.

# State of Washington

## **Month & Year End:**

The procedure for closing out the month in ctcLink involves many steps to close the submodules listed above to ensure that submodule journals post to the General Ledger Accounts in the proper order. This involves making any necessary adjustments to the sub modules before they close, viewing general ledger and submodule queries from the system to identify any issues and ensuring all journals are posted to the proper period. SBCTC maintains a "ctcLink Reference Center" website, that contains a [monthly Closing Check list](#), which lists all the required steps in order. The checklist also outlines whether the steps are done by the College, the Enterprise Resource Planning (ERP) support team or by SBCTC accounting staff.

## **Posting College General Ledger Activity to AFRS**

After all of the required month end steps have been completed by the Colleges or the ERP support team at SBCTC, Sue Willis, ctcLink Accounting Manager, performs processes using CEMLI to process the AFRS customization to crosswalk PeopleSoft distributions to AFRS. The CEMLI process maps GL attributes and agency codes using AFRS transaction codes and rules to produce an AFRS GL report to upload to AFRS using the AFRS toolbox utility.

This report is a summarized report of all data from PeopleSoft that has passed through edits for a specific month. The report is the combined table from all TBL tables from each module (as posted to the GL). The AFRS report comes directly from the General Ledger after all submodules have been closed.

The AFRS report is submitted to the Office of Financial Management (OFM) through the Axeway process. The data incorporated in this file contains only valid entries; all others remain in error files.

This report can be run as many times as necessary; but once submitted to OFM it should not be run again unless the file is protected by an archive copy.

## **Reconciliation Between the ctcLink system and AFRS**

SBCTC uses an in-house developed software program called CEMLI (pronounced kim-lee) to upload monthly data from PeopleSoft into AFRS. CEMLI has been continuously updated and improved since 2019 in an effort to make this process more efficient. The CEMLI program automatically converts College ctcLink GL data to AFRS account coding for uploading into the AFRS system **(Key Control #1 Automated - Completeness)**.

The System Accounting Coordinator reviews error reports, which identify discrepancies between the entries in ctcLink and AFRS and follows up on any coding errors and variances identified, to ensure the data reconciles between the two systems **(Key Control #2 Manual - Completeness)**.

Part of the monthly review of the reports process, is to verify that previous exceptions were corrected and all new exceptions were reported to the College involved. Generally, the Colleges will fix the incorrect entries as soon as they receive the Monthly Error Report from Sue. If it is not cleared in the following month when the next Monthly Error Reports are run, SBCTC works with the College to correct the error. Sue will mark "critical" errors she identifies during her reconciliation and follow up with the Colleges directly for some errors, but the

## State of Washington

Colleges are expected to monitor and review their monthly "SMARTER" reports to correct issues throughout the year. The SMARTER Query procedures are posted on the SBCTC [website](#).

The smarter query reports are the ctcLink version of the legacy Standard Monthly Analysis and Review of Transactions reports that were designed to test and analyze accounting data on the college level according to specific criteria. The results indicate errors that need to be corrected such as specific funds not allowed in specific ledgers, overspent capital and operating allocations, depreciation not booked, etc. The colleges are instructed to resolve smarter errors monthly and required to resolve any errors remaining at year end.

### **CEMLI Processes**

The transactions run sequentially from ACT/RVW/RPT/TBL.

Sue Willis, System ctcLink Accounting Coordinator, performs the following procedures each month:

The System ctcLink Accounting Coordinator uses pivot tables and error reports to reconcile and confirm the data input from PeopleSoft made it to AFRS for each college, for each month, without errors or variances between the amounts **(Key Control #2 Manual - Completeness)**.

The System ctcLink Accounting Coordinator, runs the "SAO Query" (also referred to as PS-SAO or SAO Zero Report) and compares it to the ACT table to ensure all of the transactions are processed by CEMLI. The SAO Query grabs all of the transactions that were keyed in PeopleSoft, without looking at the particular sub-module. The ACT table (ctc\_AFRS\_ACT\_Union) contains all of the transactions in debit/credit form, prior to the CEMLI turning them into transaction codes for AFRS. This comparison confirms that all of the transactions are processed by CEMLI.

Next, Sue reviews "Error Report 1", looking for matching errors. Between ACT & RVW, the CEMLI matches debits and credits and if it cannot find the match, it kicks them out to the error report if it is not a one-to-one match. For example, it cannot match two \$500 credits that add up to a \$1,000 debit. Corrections are usually simple and are corrected on the AFRS FT (Financial ToolBox). From RVW to RPT, the CEMLI translates the ctcLink funding source to AFRS funds. Between RPT & TBL the CEMLI verifies a transaction code is present, checks for subsidiary codes, Appropriation Indexes, etc. Anything that does not pass the tests kicks out to "Error Report 2". Sue follows up on each error and makes the necessary updates. TBL is the final table in the CEMLI process. The final data on the TBL file is placed on a server for AFRS to pick up.

One of the updates to the CEMLI process during fiscal year 2023 involved the addition of a "reconciliation balancing tool" to make this process more efficient and helps with matching debits and credits in ctcLink. Sue indicated that she rarely has much on the error reports to review now and is able to complete reconciliations for all the colleges before AFRS closes for the month.

### **Year-End Adjustments**

SBCTC reviews all potential year-end adjustments and supporting documentation to ensure they are reasonable and accurate prior to entry into

## State of Washington

AFRS during periods 132 and 133. Once all the documentation is received and reviewed, Sue Willis, ctcLink Accounting Manager, will update AFRS. After all year-end adjustments have been made, Sue will perform the reconciliation between ctcLink and AFRS, to ensure that the amounts entered in ctcLink by the individual colleges are accurately recorded in AFRS and that the balances are complete (**Key Control #3 Manual - Completeness**). If variances are identified, SBCTC will follow up with the College to ensure that the explanation for the variance is reasonable and that the adjustment in AFRS is appropriate. Any adjustments requested after close of AFRS need to be approved and made through OFM. If OFM does not approve of the adjustment, it's typically due to an error in the adjustment, such as, using incorrect funds or accounts. OFM will notify SBCTC of the error and SBCTC will reach out to the College to make the correction. Once corrected, the Colleges GL will be closed and the data will be uploaded in AFRS.

Although large improvements were made and the PeopleSoft data is being reconciled to AFRS on a regular basis, the Board has not been able to correct all of the GL beginning balances from prior year errors, so some of the information reported is still questionable. Sue Willis, ctcLink Accounting Manager, provided us with an update to the beginning balances correction process:

- Sue has created a spreadsheet to compare the ctcLink balances to the AFRS balances. Sue will identify errors using this spreadsheet.

- Sue is currently working with OFM to determine how they're going to work through the beginning balance adjustments.

- Sue will meet with OFM to propose corrections on the college level. If OFM agrees to the correction, Sue will reach out to the College to request the correction.

- OFM must approve all corrections to the beginning balances; and supporting documentation is required.

- All legacy data is maintained in a database to identify balances from prior years.

- SBCTC and OFM's goal is to have the beginning balances reconciled before the transition to OneWA.

### Key Controls are as Follows:

- Key Control #1 (Automated) - Completeness** - SBCTC uses an in-house developed software program (CEMLI) to upload monthly data from PeopleSoft into AFRS. CEMLI automatically converts ctcLink data to AFRS account coding from the college general ledgers.

- Key Control #2 Manual - Completeness: (Monthly)** - The System ctcLink Accounting Coordinator uses pivot tables and error reports to reconcile and confirm the data input from PeopleSoft made it to AFRS for each college, for each month, without errors or variances between the amounts.

- Key Control #3 Manual - Completeness: (Year end)** - After all year-end adjustments have been made, the System ctcLink Accounting Coordinator will perform the reconciliation between ctcLink and AFRS, to ensure that the amounts entered in ctcLink by the individual colleges are accurately recorded in AFRS and that the balances are complete.

### Noted Weaknesses are as Follows:

None

### J.1.PR.G - Community and Technical Colleges

# State of Washington

**Procedure Step:** Key Control #1 (Automated) - CEMLI conversion of ctcLink data to AFRS account coding  
**Prepared By:** DRR, 7/2/2024  
**Reviewed By:** BM2, 11/20/2024

## Purpose/Conclusion:

### **Purpose:**

To determine whether CEMLI automatically converts ctcLink data to AFRS account coding from the college general ledgers (**Key Control #1 for the ctcLink System Reconciliation**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Risk Assessment\]](#).

## Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

## State of Washington

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

### Automated Interfaces:

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

## State of Washington

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception*



## State of Washington

*report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

# State of Washington

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **Automated Interfaces:**

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

## State of Washington

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

### Computer Generated Reports:

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

### Electronic Approvals:

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

# State of Washington

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

## State of Washington

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

# State of Washington

## Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management,*

## State of Washington

*master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

## State of Washington

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?  
How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.



## State of Washington

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Automated Interfaces:

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) worksheet in the Store.

### Computer Generated Reports:

## State of Washington

If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.

If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.

If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance workpaper in the Store.

# State of Washington

## **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Information Technology](#) Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This

## State of Washington

process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

## State of Washington

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

## State of Washington

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An "**electronic signature**" can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A "**digital signature**" is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the**

# State of Washington

**Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

Internal controls in the ctcLink System Reconciliation process address the following balance(s):

**1. Higher Education - Special Revenue:**

- AC - Cash & Cash Equivalents
- CG - Federal Grants-In-Aid
- CH - Charges for Services
- FS - Education

**2. Higher Education - Student Services**

- AC - Cash & Cash Equivalents

**3. Governmental Activities:**

- 2C - Depreciable Assets (Net of Accumulated Depreciation)
- 2C - Education - Higher Education - Charges for Services
- 3C - Education - Higher Education - Operating Grants & Contributions
- G3 - Education - Higher Education - Expenses

For the following assertions:

- Completeness

- SBCTC: Detail roll-up from ctcLink to AFRS may be incorrect

The understanding for this system is documented above in the "Controls - ctcLink System Reconciliation" step.

**STEP 1: Understand Automated Key Control**

SBCTC uses an in-house developed software program called CEMLI to upload monthly data from PeopleSoft into AFRS. The CEMLI program automatically converts College ctcLink GL data to AFRS account coding for uploading into the AFRS system (**Key Control #1 Automated - Completeness**).

**STEP 2: Confirm and Test Automated Key Control:**

We received the data text file that CEMLI produces when converting ctcLink data to AFRS data, the Excel file that SBCTC creates to review the ctcLink transactions that have been converted to AFRS and the error report which has the ctcLink data that could not successfully convert to AFRS data SBCTC used for their February 2024 Reconciliation of peoplesoft/ctcLink data to AFRS accounts and we utilized this data for testing the

## State of Washington

automated control.

We met with Sue Willis, ctcLink Accounting Coordinator, on June 26, 2024 to walk us through the process of converting ctcLink data to AFRS data using CEMLI. Using four different queries from FM08 of FY24 data, which was screenshared via Teams by Sue, we were able to follow the process of a single ctcLink transaction being converted into an AFRS transaction.

In query one (from the ACT process) the data is in ctcLink form which had four rows of data from unit WA140 (Clark College). The first two rows were ctcLink account codes 5010040 (Medical Aid) totaling \$35.17 and the second rows were account code 5010050 (Labor & Industries) totaling \$33.12 for a combined total of \$68.29. Additionally, AFRS GL 6510 included on these lines during the conversion process.

In queries two and three (from the RVW and RPT process), the ctcLink account code is dropped and the rows are combined using the Journal ID into two rows with the first totaling \$34.06 and the second totaling \$34.23 for a combined total of \$68.29.

In query four (from the TBL process), the other AFRS GL is included which is GL 9920, and the OFM agency code is included: 635 (Clark College). Many other columns are added or broken out from prior processes and they include breaking out the fund, class, subobject MJR GRP, MJR SRC, and many more.

Lastly, Sue shared the actual AFRS entry and we noted that there were two rows of data, which included a credit of \$68.29 to GL 9920 and a debit of \$68.29 to GL 6510. Based on this walkthrough, we can confirm that CEMLI is converting ctcLink data to AFRS data. **No issues noted.**

### **STEP 3: Understand General IT Controls**

On June 5, 2024 we met with Tamara Morrill, Data Integration Developer, and Christopher Soran, Applications Support Manager, to gain an understanding of general IT controls related to CEMLI.

The version of CEMLI that is responsible for converting ctcLink data to AFRS data is separate from other versions of CEMLI and has different processes and procedures to update the program. The following information only relates to the CEMLI program responsible for ctcLink to AFRS data conversion. There have been many updates to the CEMLI program since ctcLink was implemented, but according to Christopher, the program is now in a good place and updates have not been needed since the first half of FY24.

If CEMLI program updates are needed, a ticket must be created. These tickets are typically created by Sue Willis, ctcLink Accounting Coordinator, or Teri Sexton, Director of Accounting and Business Services, however, other staff can create tickets. Tickets will be forwarded to Teri, and if she determines the program update is needed, the ticket will be forwarded to Christopher Soran, Applications Support Manager, who will review the ticket and assign a developer with the skills necessary to complete the task. The developer will develop the program changes in the PDV (development) environment. Once their development is complete, Christopher will review the work and approve the changes if it looks correct. If it doesn't look correct, Christopher will deny and send the ticket back to the developer for changes. Once approved, the changes will be migrated



## State of Washington

to the PTS (test) environment. The Quality Assurance team will review the ticket for the requirements of the changes and will test the changes in the PTS environment to ensure the changes function as intended. Once the QA team has tested the changes and determined the changes function as intended, they will forward the ticket to the Director of Application Services, who will review the ticket and will approve the migration to the PQA (Quality Assurance) environment. In the PQA environment, another round of testing will be performed by a different QA team member. If the program changes pass this round of testing, the ticket will be forwarded back to Christopher for approval and if approved, deployment to PROD (production). Once the program changes have been migrated to PROD, another review will be performed by the QA team to ensure the update is functioning as intended (**General IT Key Control #1**).

**Note:** All CEMLI program changes are logged by the system, including the name of the individual making the change and no changes can be made to the system without going through the above procedures.

### **STEP 4: Confirm Key General IT Controls**

**(General IT Key Control #1) All changes to the CEMLI system must go through a standard change process, where changes are tested, reviewed and approved before migrating to production.**

During our meeting with Tamara and Christopher on June 5, 2024 we took screenshots of the most recent CEMLI update (Tracking number - 173729). The ticket was created on August 16, 2023 and was closed on August 17, 2023. This update was to allow the system to select appropriation index by journal line date instead of sysdate within CTC\_STAFFMO2\_VW during the conversion process. We reviewed the "History" section of CEMLI which noted:

Christopher Soran, Applications Support Manager, assigned Maureen Kwant, PeopleSoft Developer & Support Engineer, the ticket on August 16, 2023.

Maureen developed the program changes in the PDV environment and submitted the changes to Christopher for review and deployment to PTS (test) environment. Christopher approved the deployment to PTS.

Joey Froehlich, Testing Coordinator, then tested the changes in PTS and forwarded the ticket to Ray Gartner, Director of Application Services, who approved deployment to the PQA (Quality Assurance) environment.

Larry Deaton performed the QA testing in the PQA and forwarded the ticket to Christopher for approval to deploy the changes to the PROD (production) environment. Christopher approved the deployment to the PROD environment.

Joey performed the last of the QA testing in the PROD environment and the ticket was closed.

**No issues noted.**

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **J.1.PRG - Community and Technical Colleges**

# State of Washington

*Procedure Step:* Key Control #2 (Manual) - Monthly Consolidation & Reconciliation  
*Prepared By:* DRR, 6/10/2024  
*Reviewed By:* BM2, 11/20/2024

## Purpose/Conclusion:

### **Purpose:**

To confirm the System ctcLink Accounting Coordinator uses pivot tables and error reports to reconcile and confirm the data input from PeopleSoft made it to AFRS for each college, for each month, without errors or variances between the amounts to AFRS (**Key Control #2 for the ctcLink System Reconciliation**) in order to assess control risk.

### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

**Step 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

List the financial statement line item(s) and relevant assertion(s) addressed by the understanding.

1. Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

A walk-through of a transaction is considered the most effective way of corroborating your understanding of internal controls .Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.

Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the

## State of Washington

person performing the control.

When a key control is discovered to not actually be placed in operation, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If a key control is automated, the confirmation of our understanding should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

If a key control is not consistently or effectively applied, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.

If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.

If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "Key Control - Automated" step. Auditors should consider contacting Team IT Audit for assistance.

## State of Washington

An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of State-Level control elements. In doing so, all of the following specific determinations must be documented:

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.
- B. Controls are not related to a "significant risk" identified in the audit plan.
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

### **Material Balance(s) and Assertions**

Internal controls in the ctLink System Reconciliation address the following balance(s):

#### **1. Higher Education - Special Revenue:**

- AC - Cash & Cash Equivalents
- CG - Federal Grants-In-Aid
- CH - Charges for Services
- FS - Education

#### **2. Higher Education - Student Services**

# State of Washington

AC - Cash & Cash Equivalents

## **3. Governmental Activities:**

2C - Depreciable Assets (Net of Accumulated Depreciation)

2C - Education - Higher Education - Charges for Services

3C - Education - Higher Education - Operating Grants & Contributions

G3 - Education - Higher Education - Expenses

For the following assertions:

Completeness

SBCTC: Detail roll-up from ctcLink to AFRS may be incorrect

## **Key Control #2 - Manual, Completeness: (Monthly)**

The System ctcLink Accounting Coordinator uses pivot tables and error reports to consolidate, reconcile and confirm that the data input from PeopleSoft made it to AFRS for each college, for each month, without errors or variances between the amounts.

The understanding for this system is documented above in the "Controls - ctcLink System Reconciliation" step.

## **1. Confirmation of Key Manual Control:**

Note: SBCTC uses the terms PeopleSoft and ctcLink interchangeably.

We requested and received SBCTC's February 2024 reconciliation of ctcLink to AFRS data from Sue Willis, ctcLink Accounting Coordinator. During our review of the February 2024 reconciliations, we noted that all corrections had notes to explain why the correction was made. Most of these corrections were due to an invalid GL account/fund combination. There were additional corrections marked as "Correction Returns" or "Ledger Correction" which are errors identified by SBCTC using their exception reports or manual review. These types of errors are sent back to the College for correction.

We noted that all 30 Colleges and SBCTC (total of 31) were included in the February 2024 reconciliation. Additionally, we noted the total revenue (GL32XX) and total expenses (GL65XX) reconciled without exception. We confirmed that SBCTC is consolidating, reconciling and confirming the data input from ctcLink is making it to AFRS without errors or variances between the amounts. **No issues noted.**

## **Noted Weaknesses are as follows:**

None.

## **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

# State of Washington

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

#### **J.1.PR.G - Community and Technical Colleges**

*Procedure Step:* Key Control #3 (Manual) - Year End Consolidation & Reconciliation

*Prepared By:* DRR, 10/9/2024

*Reviewed By:* BM2, 11/20/2024

#### **Purpose/Conclusion:**

##### **Purpose:**

To confirm after all year-end adjustments have been made, the System ctcLink Accounting Coordinator will perform the reconciliation between ctcLink and AFRS, to ensure that the amounts entered in ctcLink by the individual colleges are accurately recorded in AFRS and that the balances are complete (**Key Control #3 for the ctcLink System Reconciliation**) in order to assess control risk.

##### **Conclusion:**

We noted **no** material weaknesses or significant deficiencies in internal controls.

#### **Testing Strategy:**

##### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption [RCW 42.56.420](#) for cyber security purposes. The details documented in the record of work and supporting workpapers may qualify for this exemption. Auditors must include this statement in workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited."**

## State of Washington

**Steps 1 and 2 are required as part of the auditor's understanding of controls and must be done even if the auditor plans to assess control risk for the system at MAXIMUM. Step 3 is only required if the auditor plans to assess control risk for the system at LOW.**

**Auditors should consider contacting Team IT Audit to discuss any questions or concerns related to the automated control and to determine if the use of an IT Specialist is needed. Team IT Audit can assist in developing a specific testing strategy, performing test of controls, or evaluating results and how they will affect the audit.**

The understanding of the automated control should be documented in the internal control write-up of the system. The write-up should reference this step as the confirmation and testing of the identified automated key control and any relevant General IT Controls.

1. Develop a specific testing strategy to determine if the automated control is in place and operating as designed. The objective of the automated control test is to determine whether the software calculation control correctly values each transaction taking into consideration variations due to situational differences.

An automated control will function consistently unless the program is changed (including the tables, files, or other base data used by the program). Controls over the integrity of the program and data are referred to as "general controls." Because of this inherent difference between computers and people, our audit approach to confirming and testing automated controls is different than for manual controls.

Due to this inherent consistency, confirming an automated control is in place also counts as a test of effectiveness. Also, only one instance of the automated control would need to be tested for each variation of the control. However, to set control risk to LOW, general controls would also need to be tested to provide evidence of the consistent operation of automated controls.

If the expected automated control is not in place or operating effectively, the auditor should consider whether a significant deficiency or material weakness in controls over financial reporting exists.

2. Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls.

A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or

## State of Washington

detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Guidance/Criteria tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency.

**All potential material weaknesses and significant deficiencies must be discussed with the AIC, since they must be reported as findings.**

3. If the auditor plans to set control risk at LOW, develop a specific testing strategy and test general IT controls related to the automated control (otherwise, this step would not need to be performed). The objective of the general IT controls test is to determine whether security and program change controls support consistent implementation of key automated (application-level) controls.

General IT Controls are higher-level controls that maintain the integrity of the automated controls and data storage. Entity size, organizational structure, sensitivity, and importance of the data will affect the types of General IT Controls tested and the level recommendation. Keep the focus of General IT Controls at the application level associated with the automated control.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies are deemed a material weakness if it caused an exception with the compliance requirement or assertion. If general IT controls are not effective, we cannot rely on the automated control to reduce control risk to LOW.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Information Technology](#) Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material**



# State of Washington

**Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

## **Significant Balance(s) and Assertions**

Internal controls in the ctcLink System Reconciliation process address the following balance(s):

### **1. Higher Education - Special Revenue:**

- AC - Cash & Cash Equivalents
- CG - Federal Grants-In-Aid
- CH - Charges for Services
- FS - Education

### **2. Higher Education - Student Services**

- AC - Cash & Cash Equivalents

### **3. Governmental Activities:**

- 2C - Depreciable Assets (Net of Accumulated Depreciation)
- 2C - Education - Higher Education - Charges for Services
- 3C - Education - Higher Education - Operating Grants & Contributions
- G3 - Education - Higher Education - Expenses

For the following assertions:

Completeness

SBCTC: Detail roll-up from ctcLink to AFRS may be incorrect

### **Key Control #3 Manual - Completeness:**

After all year-end adjustments have been made, the System ctcLink Accounting Coordinator will perform the reconciliation between ctcLink and AFRS, to ensure that the amounts entered in ctcLink by the individual colleges are accurately recorded in AFRS and that the balances are complete.

The understanding for this system is documented above in the "Controls - ctcLink System Reconciliation" step.

## **2. Key Manual Control Confirmation:**

# State of Washington

We met with Sue Willis, SBCTC System ctcLink Accounting Coordinator, on October 7, 2024 to walk through her year-end ctcLink to AFRS reconciliation of the consolidated Agency 699 general ledger data for all 30 Colleges and the SBCTC. Sue provided us with several large excel files and a word document that contained notes about the consolidated data and the reconciliation she performed during the month of September 2024. Sue reconciled Consolidated College & SBCTC General ledger data by GL, Fund, and source of revenue and subobjects as outlined below.

## **Year End Data Consolidation & Reconciliation Process:**

### ctcLink Data

Sue Willis, SBCTC System ctcLink Accounting Coordinator, uses query "QFS\_GL\_ACCT\_ANALYSIS\_ATTR" to obtain ctcLink data. Due to the large size of the query, this is query is run six times and each query includes the following units:

- WA000-WA050
- WA060-WA100
- WA110-WA150
- WA160-WA200
- WA210-WA250
- WA260-WAPAY

AFRS reporting periods for the ctcLink data are 1-132. Sue adds a SRC (source) column as a data identifier "PS-LEDGER" to show that this data is from ctcLink. She then filters the sub-object column to exclude blanks, and the appropriation index is filtered from down to blanks. She then filters the fund column to remove any state allocated fund entries, 997 and 999. Next, she creates three pivot tables in each of these spreadsheets. These pivot tables are copied into three additional spreadsheets and will be combined with AFRS data to allow for comparison of GL, GL-Revenue and GL-Sub-Object data.

### AFRS Data

Sue runs a data extract in AFRS to pull batches BE, KC, RC, SW, and X1 as these are the AFRS entries that correspond to the ctcLink reconciliation data. She adds a SRC (source) column as a data identifier "AFRS" to show this data came from AFRS. Agency, PS-Unit, REV columns created to match ctcLink data elements. GL71xx is changed in the "GL\_account" column to GL 1110 to match ctcLink data pull. Three pivot tables are created to match the same data elements as the ctcLink data.

### Combining ctcLink and AFRS data

Sue then creates three data sets (Revenue, Expenditure, Combined GL) by combining the eighteen pivot tables of ctcLink data, and the single AFRS spreadsheet. Sue mentioned that variances in the combined data were limited to the following:

- PS-GL1350 needed to be adjusted to GL1312 in AFRS
- PS-GL5150 needed to be adjusted to GL5111 in AFRS
- PS-Fund 148 GL1440 needed to be adjusted to Fund 148 GL1410 in AFRS
- PS-Fund 790 GL32xx needed to be adjusted to Fund 790 GL5199 in AFRS

## State of Washington

PS-Fund 790 GL65xx needed to be adjusted to Fund 790 GL5199 in AFRS  
PS-Fund 790/840 GL1383 need to be adjusted to Fund 790/840 GL1319 in AFRS  
PS-Fund 790/840 GL5190 need to be adjusted to Fund 790/840 GL5111 in AFRS

Sue mentioned that these variances are expected due to intentional crosswalk of data to AFRS. In the "AFRS v PS combined GL" reconciliation we noted that Sue made the various adjustments noted above and after these adjustments, there were no variances between ctcLink and AFRS data.

*We determined that SBCTC is consolidating and reconciling the ctcLink General Ledger data by fund with AFRS balances at year end, and working directly with OFM to resolve differences before the AFRS adjustment periods close.*

### Noted Weaknesses are as follows:

None.

### **2. Preliminary Control Risk Assessment**

Based on our understanding and anticipated audit strategy, we assessed preliminary control risk as follows:

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **3. Control Risk at LOW - Test of Key Manual Control:**

Not applicable - we are not planning to rely on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **J.1.PRG - Community and Technical Colleges**

*Procedure Step:* Risk Assessment

*Prepared By:* DRR, 7/19/2024

*Reviewed By:* BM2, 11/20/2024

Purpose/Conclusion:
---------------------

**Purpose / Conclusion:**

# State of Washington

To assess inherent risk, control risk, and the risk of material misstatement in order to design an initial testing strategy for each assertion.

Testing Strategy:

Auditors are **required** to perform the following procedures for each line item:

## **STEP 1: Inherent Risk (IR)**

Assess inherent risk for each relevant assertion. This assessment is based on understanding of the entity and the nature of the account balance or class of transactions.

*Inherent risk is the susceptibility of an assertion to material misstatement. It is our assessment of "total threat", which includes both "natural risk" and identified risk indicators, without any regard to any potential control activities. As inherent risk is fully independent of control risk, any understanding of controls cannot be used to increase/decrease the assessment of inherent risk. Consider the following factors as your basis for this assessment:*

### *General Considerations*

*Does the balance include transactions that are difficult to audit or involve complex accounting issues?*

*Were there significant misstatements identified in previous audits or prior-period adjustments in the account balance or transaction class? If so, analyzing the cause of prior period misstatements will help in analyzing inherent risk.*

*Are there any inherent risk factors at the entity or industry level, such as changes in regulation or accounting rules, unique transactions or accounting practices, use of information technology, etc that affect the balance?*

### *Inherent Risk due to Error*

*How large are the transactions making up the balance? If the balance has only a few large transactions, even a single error may mean a significant misstatement.*

*Have there been changes in the transactions making up the balance that may increase risk? For example, significantly different composition, nature or volume of transactions may inherently disrupt established controls.*

*Are financial events originated or identified by accounting personnel or non-accounting personnel? This consideration is mainly for the completeness assertion.*

*Does the process to account for transactions involve judgment or estimation, complex calculations, numerous steps or significant manual steps?*

*Do transactions have widely varying attributes that need to be manually identified? For example, grant loans that are accounted for in one of several ways depending on the terms of the agreement.*

### *Inherent Risk due to Fraudulent Reporting (intentional misstatements)*

*Are there substantial pressures or motivations to misstate the balance?*

### *Inherent Risk due to Misappropriation*

*Is the account balance or transaction class susceptible to sizable misappropriation?*

# State of Washington

## *Inherent Risk due to Non-Compliance*

*Are there any laws, contracts or grant agreements affecting the balance? If so, would non-compliance lead to sizable misstatements?*

*Are compliance requirements complex, hard to understand, subject to judgment or otherwise difficult to comply with?*

*Are there any motivations or pressures to not comply?*

## **STEP 2: Control Risk (CR)**

Assess control risk by system and assertion. This assessment should be based on the results of the control understanding, confirmation, and (if setting control risk to LOW) testing. If applicable, auditors will evaluate any control deficiencies and determine whether those deficiencies, individually or in combination, are significant deficiencies or material weaknesses.

*Control risk is the risk that material misstatements would not be prevented or detected timely by the system of internal control. Control risk could be thought of as the "vulnerability" of an entity to misstatements. Control risk exists independently of the inherent risk (the level of vulnerability exists independent of the level of threat).*

*Control risk is MAX in both of the following situations: (1) controls aren't tested or (2) controls are problematic and cannot be relied upon. In order to set control risk to LOW, the auditor must test that controls operated effectively throughout the period.*

*A material weakness exists when the design or operation of controls results in a reasonable possibility a material misstatement will not be prevented or detected and corrected in a timely manner. A significant deficiency is less severe than a material weakness, yet important enough to merit the attention of the governing body. **All potential material weaknesses and significant deficiencies should be discussed with the AIC, since they must be reported as findings.***

## **STEP 3: Risk of Material Misstatement (RMM)**

Assess the risk of material misstatement for each relevant assertion for each significant line item. The risk of material misstatement (RMM) is a combination of the auditor's separate assessment of inherent and control risk.

*In practice, the RMM is the amount of substantive evidence that's needed, and the only way to reduce the amount of needed substantive evidence (equal to the inherent risk) is to test controls. As such, when control risk is MAX, the RMM must always equal the inherent risk (IR).*

*When controls are tested & can be relied upon (are determined to be effective) it is a matter of professional judgment how much the RMM should be set lower than inherent risk (1 or 2 steps).*

*Auditors should assess RMM by assertion, if different. For example, if RMM is assessed at MOD for the existence assertion, but LOW for the rights & obligations assertion, then document "MOD – existence and LOW – rights & obligations".*

# State of Washington

## **STEP 4: Design Substantive Testing**

Design a substantive testing strategy that addresses the relevant assertion (identified risk) in the portion of the line item that relates to that risk.

*Planning identifies where to audit (significant balances, classes of transactions & disclosures) what to audit for (relevant assertions), and how much to audit (RMM). The quantity and quality of evidence obtained by substantive tests needs to match the level of risk. The higher the risk of material misstatement, the greater evidence needed. "Greater evidence" could either be greater quantity of evidence, greater quality of evidence, or some combination of greater quality and quantity.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6210](#) – Planning Financial Statement Audits**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits Planning Guide](#)**

Record of Work Done:

## **(1) Inherent Risk (IR):**

Based on our understanding of the line item, we assessed inherent risk as follows for each relevant assertion and significant class of transactions:

Completeness – **High**

## **(2) Control Risk (CR):**

We assessed control risk as follows for each system and relevant assertion:

**ctcLink System:** A reconciliation is performed to ensure that consolidated college & SBCTC financial data uploaded from ctcLink is complete, properly valued and recorded into AFRS correctly.

Completeness – **MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **(3) Risk of Material Misstatement (RMM):**

## State of Washington

We considered both inherent and control risk and assessed the risk of material misstatement as follows for each relevant assertion and significant class of transactions:

Completeness – **High**

### **(4) Testing Strategy:**

We designed our substantive testing strategy based on our assessment of the risk of material misstatement. We plan to perform the following tests:

We will use SBCTC's reconciliations to ensure that all 30 colleges and all accounting periods are included in the reconciliations.

We will reperform SBCTC's reconciliation by using the ctcLink activity and comparing it to our Access (AFRS) database.

We will use specific college source data and compare it against the SBCTC reconciliation data to determine if it is reasonable.

We will review the Exception Reports for balances specifically related to SBCTC

We anticipate that these tests will provide sufficient appropriate audit evidence to address the assessed risk of material misstatement for relevant assertions in significant classes of transactions.

### **J.1.PR.G - Community and Technical Colleges**

*Procedure Step:* Substantive Test

*Prepared By:* DRR, 11/15/2024

*Reviewed By:* RKM, 11/19/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To determine if there are unexplained variances between AFRS and amounts reported by SBCTC from ctcLink Systems (**Completeness**).

### **Conclusion:**

We determined that consolidated year end reconciliation amounts for colleges and the SBCTC agree to AFRS agency 699 totals. No issues with the SBCTC reconciliation amounts were noted, however we identified the following issue:

We identified questionable balances related to SBCTC during exception report review. **See issue here:** [[E: SBCTC Questionable Balances](#)]. **See AOM here:** [[Aggregation of Misstatements \(GAAP\)](#)]

# State of Washington

## Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

*Note: intergovernmental revenues received from the State Treasurer should be addressed as part of the State Treasurer Distributions baseline test.*

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

### **Cut-Off / Revenue Recognition**

Test transactions recorded in the current period to verify the revenue occurred during the period.

*Transactions recorded at the beginning and end of the current period would generally be considered at highest risk of being improperly recorded in the current period. Consider scanning and selecting transactions if high risk transactions can be identified by description or date fields.*

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

### **Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

### **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at*



## State of Washington

*the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Calculation**

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

### **Realizable Value**

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### **Estimation / Recognition**

Review calculation and support for assumptions of any estimated revenues.

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

### **Property Tax Revenues** - see separate step

Guidance/Criteria:

**Add the Guidance/Criteria for each relevant assertion from the TeamStore. You may also include other resources that you used for testing.**

Record of Work Done:

Note: SBCTC only consolidates and reconciles college activity for the current fiscal year between ctLink and AFRS.

### **Substantive tests performed to meet the Completeness assertion:**

## State of Washington

To test for completeness [[ctcLink to AFRS Data Reconciliation Testing](#)], we used AFRS data that SBCTC used in their ctcLink to AFRS reconciliation, which was provided to us by Sue Willis, ctcLink Accounting Coordinator. We created a pivot table by ctcLink business unit which is how the colleges are identified in ctcLink and noted that there were 30 colleges included in the data. Additionally, we used SBCTC's AFRS data extract file "2\_24.09.18\_AFRS-BE\_KC-RC-SW-X1 Batch.xlsx." to create a pivot table by fiscal months to ensure that SBCTC was including all accounting periods (1-12 & 99) from the fiscal year in their data. **No issues noted.**

Additionally, we reperformed SBCTC's reconciliation [[ctcLink to AFRS Data Reconciliation Testing](#)], and gained an understanding of the various adjustments that SBCTC made to college GL data. Per Sue Willis, ctcLink Accounting Coordinator, she worked with Kelly Diaz, Statewide Accounting Supervisor to determine how to address the various GLs that are used in ctcLink but not in AFRS, and how some funds don't work for recording various transaction types. Sue provided us the following explanations:

- GL1350 and 5150 were used in the legacy system (FMS) to record due to/due from for state funds. It was determined that it would be best to move all balances for these two GL accounts in AFRS to 1312 and 5111. As colleges clear the balances in 1350/5150 that may remain in ctcLink, SBCTC hits either 1312 or 5111 which will zero out any remaining balances in AFRS.

- Fund 148 would not allow for the recording of GL1440. Sue worked with Kelly Diaz at OFM to determine that GL1410 would be the best GL to report these transactions in.

- GL32xx transactions are not permissible in Fund 790. These transaction should be moved to another GL, or refunded within a limited time period. It was determined that these transactions should be moved to GL5199 to avoid the creation of equity entries.

- GL65xx transactions are not permissible in Fund 790. These transaction should be moved to another GL, or refunded within a limited time period. It was determined that these transactions should be moved to GL5199 to avoid the creation of equity entries.

- GL1383 and 5190 transactions are not permissible in Funds 790 or 840. It was determined that moving these transactions to GL 1319 and 5111 would be the best solution to allow for reporting a receivable/payable for these two funds.

During our reperformance of the SBCTC reconciliation, we confirmed that the adjustments SBCTC made were reasonable. **No issues noted.**

We also pulled QFS\_GL\_ACCT\_ANALYSIS reports from ctcLink for two selected colleges (Centralia College [[Centralia Source Data Testing](#)] and Tacoma Community College [[Tacoma CC Source Data Testing](#)]) and Columbia Basin [[Columbia Basin Source Data Testing](#)] (due to an error identified in the FY23 ACFR) to compare source data amounts of various GLs against the SBCTC reconciliation data. To prepare the source data for comparison against SBCTC's data, we used the Vlookup function to add AFRS GLs to the data, removed fund 790 data for revenue and expenditures, which was adjusted to GL5111, and changed ctcLink fund 146 to fund 145. These changes are made so that the ctcLink data, can match how the data is recorded in AFRS.

We created pivot tables of GL1110, 3210, 6510 and capital assets (GL2210-2440) using our source data for each of these colleges and compared it to the data provided in SBCTC's reconciliation. Our GL totals tied to SBCTC's totals without exception. **No issues noted.**

Exception Report Balances for SBCTC [[SBCTC Exception Report Balances](#)]

## State of Washington

We identified exception report balances for SBCTC at N.4.7, N.4.19 and N.4.20. We requested Kennesy Cavanah, Statewide Accountant, provide an explanation of these balances. We identified the following questionable balances related to SBCTC:

### Assets with Credit Balance:

Fund 450 GL 1110 Cash in Bank (\$4,954,749.58). Per Kennesy Cavanah, Statewide Accountant, This balance should have been zeroed out at fiscal year end and should be cleaned up during FY25. **See issue in conclusion.**

Fund 790 GL 1318 Unbilled Receivables (\$1,641,145.88). Per Kennesy Cavanah, Statewide Accountant - Part of beginning balance cleanup that is the focus for FY25. **See issue in conclusion.**

Fund 859 GL 1110 Cash in Bank (\$2,148,656.02). Per Kennesy Cavanah, Statewide Accountant - Part of beginning balance cleanup that is the focus for FY25. **See issue in conclusion.**

### Liabilities with Debit Balance:

Fund 145 GL 5181 Employee Insurance Deductions Payable \$1,922,085.18. Per Kennesy Cavanah, Statewide Accountant - Part of beginning balance cleanup that is the focus for FY25. **See issue in conclusion.**

Fund 846 GL 5190 Unearned Revenues \$1,596,203.80. Per Kennesy Cavanah, Statewide Accountant - Part of beginning balance cleanup that is the focus for FY25. **See issue in conclusion.**

### Comparison of Reconciliation Data to Community College Access Database (AFRS) [[ctcLink to AFRS Data Reconciliation Testing](#)]

We compared SBCTC reconciliation data provided by Sue Willis, ctcLink Accounting Coordinator to our community college Access database (data found here [[Final Planning Community Colleges Selected for Testing](#)]) to determine if the reconciliation data tied to our AFRS data in the database. We determined that we would look at 71% of the balance to ensure we had sufficient coverage of the balances.

We pulled the itemized AFRS data from B.3.2 for the following income statement balances: Charges for Services - Fund Level, Charges for Services - Government Wide, Education Expense - Fund Level, Higher Education Operating Grants and Contributions Government Wide and used the itemized data to filter the reconciliation data provided by SBCTC for our comparison. We determined that the reconciliation data in these balances ties to AFRS. **No issues noted.**

Additionally, we pulled the itemized AFRS balance sheet data for Cash & Cash Equivalents, and Depreciable Capital Assets. As the SBCTC reconciliation data only includes FY24 activity, we also pulled the community college FY23 ACFR data for these balances and subtracted them from the FY24 data. This gave us the AFRS activity for these balances, which we compared to the activity for these balances in SBCTC's reconciliation data. The activity in AFRS tied to the reconciliation activity without exception for Cash & Cash Equivalents and tied with a variance below the floor for Depreciable Capital Assets. **No issues noted.**

### J.1.PRG - Community and Technical Colleges

# State of Washington

*Procedure Step:* Scholarship Allowance Assessment  
*Prepared By:* RKM, 12/6/2024  
*Reviewed By:* SHW, 12/17/2024

Purpose/Conclusion:

Testing Strategy:

Document our assessment related to the scholarship allowance exception.

Guidance/Criteria:

Record of Work Done:

## **Overview:**

Scholarship discounts and allowances are the difference between the stated charge for the goods and services provided by a college or university and the amount that was paid by the students or third parties making payments on the student's behalf. We determined that OFM was not including this allowance in the Statement of Revenues, Expenses and Changes in Net Position and the Statement of Activities. Student tuition and fee revenues and certain other revenues from students, should have been reported net of scholarship discounts and allowances.

We spoke with Anna Quichocho, Financial Reporting Manager, on November 6, 2024 to discuss this issue. She agreed that OFM needed to include this part of the statements and provided us the worksheet adjustment that OFM made to include the allowance. See: [\[RE Scholarship Allowance\]](#). In fiscal year 2024 the Office of Financial Management (OFM) estimates state colleges and universities had \$552 million in scholarship discounts and allowances. We decided to perform analytical procedures over this estimate and determine if there is a potential risk of material misstatement.

We met with Anna on November 19, 2024 to determine the methodology OFM used to estimate the allowance. Anna prepared the estimated by performing the following steps:

Contacted UW and WSU to determine whether there was an estimate posted in AFRS. UW posted the estimate to the incorrect fund and WSU did not post one at all.

## State of Washington

She ran a query to obtain tuition revenue (GL 3205/3210 and source 0424) data. She used this data to determine the allocation between government-wide (93.62%) and proprietary (6.38%) on the financial statements.

Due to time constraints she utilized the most recent estimate the college reported on their financial statements (excluding UW and WSU). She used the percentages to allocate the estimate between government-wide and propriety on the financial statements.

This was the impact before OFM's estimated corrections:

Higher Education Special Revenue Fund - Charges for services were understated and education expenditures were understated by \$189 million.

Higher Education Student Service Fund - Charges for services were overstated and miscellaneous expenses were overstated by \$35 million.

Governmental Activities - Charges for services were overstated and higher education expenses were overstated by \$327 million.

Business-Type Activities - Charges for services were overstated and higher education student services expenses were overstated by \$35 million.

### **Overview:**

Planning analytical procedures for FY24 consisted of updating the multi-year trend analysis with FY23 information (FY24 data is not available at the time of interim planning) and scanning it for unexpected differences. We also scanned the FY23 financial statement and notes for obvious errors, omission or inconsistencies, deviations from general expectations, and transactions or activity that appears inherently high risk.

### **Details:**

OFM developed a spreadsheet to show how they came up with their reported allowance estimated. The spreadsheet showed OFM used the most recent allowance the college or university reported. We utilized this spreadsheet and added a percent change in balance and year over year average percentage change (used 3 years if the amounts were available). During our analytical procedures we assessed the following:

Did OFM include all colleges and universities in the estimate?

We scanned the fluctuations for increases or decreases that would present a potential risk of material misstatement.

Compared 2024 and 2023 allowance estimates reported by colleges and universities to the total estimate reported by OFM.

### **Results:**

See spreadsheet at: [\[Scholarship Allowance Assessment\]](#).

Through our assessment we determined:

OFM included all colleges and universities in the estimate.

Estimates change year over year so the increases or decreases and the year over year averages did not alert us of a potential risk of material misstatement.

48% of the OFM allowance estimate was from amounts reported by colleges and universities in 2024 and 33% of the OFM allowance estimate was from amounts reported by colleges and universities in 2023. 81% of OFM's estimate was from the two most current years.

# State of Washington

See issue and AOM links in conclusion above.

## J.2.PR.G - Community & Tech College Testing - Seattle

*Procedure Step:* Summary & Conclusion

*Prepared By:* EZM, 10/29/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion:

**Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

**Conclusion:**

We determined that **no** modifications were necessary to inherent risk, control risk or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Significant Balance** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and*

# State of Washington

*documented in detail in the [Changes to FS Audit Plan](#) step.*

**2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:**

**Information to be used as audit evidence:**

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

**Results:**

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

# State of Washington

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

**[Investments](#) area guide**

Record of Work Done:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We noted no results from our substantive tests which would indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We determined that the quality and quantity of evidence obtained was both sufficient and appropriate.

## **J.2.PRG - Community & Tech College Testing - Seattle**

*Procedure Step:* Cash and Cash Equivalents - Controls

*Prepared By:* MRF, 9/12/2024

*Reviewed By:* CJG, 11/6/2024

Purpose/Conclusion:



# State of Washington

## **Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

## **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls. The college had not performed a year end reconciliation of the petty cash/change funds. See issue here [[V: Seattle Colleges Complete and Timely Cash Reconciliations](#)].

## Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

## **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

**Expected key control for existence and completeness:** Bank reconciliations are performed timely on at least a monthly basis to ensure the general ledger agrees to bank and investment account records.

# State of Washington

*Documentation should include who performs bank reconciliations, how often they are performed and how reconciliations are aggregated and compared to the general ledger.*

*Note: we would expect additional key controls if the government has any alternative investments or investments subject to significant interest rate or other risks.*

## Expected compensating controls:

An accounting system module or a standard template is used to document reconciliations.

Segregation of duties in that the person performing bank reconciliations does not have cash handling duties or access to initiate disbursements by wire or check.

Timely, independent review of bank reconciliation documentation, including journal entries for adjustments identified from the bank statements (such as fees, NSF checks, etc).

An up-to-date listing of change fund, petty cash and imprest fund accounts is maintained in accordance with BARS 3.8.8.

Zero-balance bank accounts and clearing funds (see BARS 3.8.6) are reconciled to zero on a monthly basis.

If the government has an investment account (that is, other than the State or County LGIP), documented inquiry with their investment service to verify the methodology for determining fair value of investments and the valuation input hierarchy level for purposes of their fair value (GASB 72) disclosures.

*Some investment accounts provide information about its methodology, assumptions, and data in valuing investments at the asset class level. However, brokers often provide no, or only limited, information about the inputs and assumptions used in developing the fair value. Management should either obtain a document with this information or contact the broker/institution to gain an understanding of the information about methods and inputs used in determining the fair value and where the investment should be disclosed in the hierarchy.*

*Contact the Investment Specialist for any questions on expected controls or documentation over fair value disclosures.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the*

## State of Washington

*manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*Suggested confirmation for expected key controls are to obtain and scan all year-end bank reconciliations and supporting documentation. This is normally done in conjunction with substantive testing. We would expect that bank reconciliations would clearly show check figures that compare the aggregated adjusted bank balance to the general ledger.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

### **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

## State of Washington

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

# State of Washington

Record of Work Done:

## **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Higher Education Special Revenue Fund - Cash and Cash Equivalents - Existence

Higher Education Student Services Fund - Cash and Cash Equivalents - Existence

See lead sheet here: [\[Lead Sheet\]](#)

## **STEP 1: Gain an Understanding of Internal Controls**

We met with David Williams (Director of Financial Reporting), Kyoko Connolly (Senior Accountant), and Charlene Rios (Director of Accounting) on September 11, 2024 to discuss the bank, cash, and investment reconciliation process at Seattle Colleges.

We noted the following accounts for cash and investments:

Bank of America. The BOA account holds their main operational flow of revenues and expenditures.

US Bank. The US Bank account only holds the proceeds from a recently matured bond investment.

Local Government Investment Pool. The LGIP statement is separate from other investment accounts.

Petty Cash/Change Fund. Physical cash at several locations used as change funds for college services.

## **Cash & Bank Reconciliation:**

Ctclink has a daily reconciliation process, but a formal review and analysis only happens once a month due to its complexity. Each month the Senior Accountant, Kyoko Connolly, downloads the online bank statement from BOA as an excel document. Kyoko also downloads the Student Financials (SF), Accounts Receivable (AR), and Accounts Payable (AP) modules in ctcLink. Kyoko uses monthly GL Queries filtered by month to compare GL Account 1000070 (cash in bank) to the information in the bank statement transaction by transaction (**Key Control #1 - Existence**). The student financial module has the most transactions to reconcile to and they do this by item type because a single deposit may be broken into multiple smaller parts because there are three colleges to track. Kyoko compares the amount per their records to the amount per the bank for each type, and any variances identified are reported back to the department responsible for adjustments, and to correct the balance. It often takes months to perform the complete reconciliation, but once done, Kyoko sends the support to Davina Fogg, Comptroller, for a review and electronic signature.

## **Investment Reconciliation**

Kyoko Connolly downloads the investment statements from the respective websites for the LGIP investments and the bond investment through US Bank. In FY24, the bond had matured in 2022 and no activity other than interest occurs in the account. At the end of the fiscal year, Kyoko

## State of Washington

compares the statement balances in the cash and investment process to ensure it is continuing as expected (**Key Control #2 - Existence**).

### **Petty Cash Reconciliation:**

Kyoko Connolly requests the cash balance reports annually from each department that has petty cash/change funds on hand. There are eight cash locations across the three campuses. Kyoko will compare these balances to what is recorded in the GL. If there are variances, she will research the cause and make adjustments to correct the differences (**Key Control #3 - Existence**).

### **Key Controls:**

Key Control #1: The finance department confirms the existence and balance of the cash account at Bank of America by performing a monthly reconciliation. This reconciliation is reviewed and signed by the Comptroller.

Key Control #2: The finance department confirms the existence and balance of the investment accounts at US Bank and the LGIP at the end of the fiscal year by reviewing the account statements.

Key Control #3: The finance department confirms the existence of the petty cash/change funds by reviewing the balances of each fund holder across the three colleges at the end of the fiscal year.

### **Identified Weaknesses:**

Due to the length of time needed to perform the monthly reconciliation, Kyoko stated the fiscal year end reconciliation has not been completed. She anticipates it being ready for auditors on October 7th, 2024. Kyoko provided the June reconciliation on October 4th, 2024. We recommend the college ensure timely reconciliations of cash and GL accounts (monthly, as required by SAAM 85.50.40.c).. See issue here [[V: Seattle Colleges Complete and Timely Cash Reconciliations](#)].

## **STEP 2: Confirm Key Controls**

**Key Control #1: The finance department confirms the existence and balance of the cash account at Bank of America by performing a monthly reconciliation. This reconciliation is reviewed and signed by the Comptroller.**

We reviewed the reconciliation for December 2023 and Jan 2024. Due to staff shortages, Kyoko often reconciles two months at a time. Kyoko provided her spreadsheet which detailed the reconciliation from the bank statement, to data pulled in the system and other reconciling items. The "header" tab had a summary of amounts linking to other sheets in the workbook, such as Deposits in Transit. The bank statement had a final balance of \$10,622,338.34. There were -\$1,078,314.55 and +\$13,800.00 in checks outstanding, and -\$55,534.44 in DIT for an adjusted total of \$9,502,289.35. Kyoko also balanced from the GL to the bank by pulling the previous balance per book, and including other reconciling items. There was a variance of \$425,549.74, which linked to the "variance" tab, where each part of the variance was broken down, investigated and resolved. After that, the true difference was listed as \$0.00. Kyoko also provided the PDF of the summary page where she signed attesting to the reconciliation on 08/30/2024 and it was reviewed and approved by the controller Davina Fogg. *No issues noted.*

**Key Control #2: The finance department confirms the existence and balance of the investment accounts at US Bank and the LGIP at the end of the fiscal year by reviewing the account statements.**

## State of Washington

We reviewed the "2024\_12 JUNE REC" workbook provided by Kyoko Connolly. The year end reconciliation packet is an excel workbook with separate tabs breaking down the balance for various types of funds, and tied to the header summary on the first tab. The digital statements were included in the reconciliation packet. The LGIP account information was pulled on 07/16/2024 and had a net ending balance of \$46,052,559.41. We also reviewed the US Bank digital statement which was physically mailed to the college and scanned in for their records. We noted an ending balance of \$2,522,800.32 which included the \$186.10 deposit in interest earned. The college does not sign the individual statements and instead includes them in the reconciliation signature for the entire packet, which was signed by Kyoko Connelly and Davina Fogg (Executive Director of Finance) on 10/03/2024. *No issues noted.*

### **Key Control #3: The finance department confirms the existence of the petty cash/change funds by reviewing the balances of each fund holder across the three colleges at the end of the fiscal year.**

As part of our testing we reviewed the year end "2024 Petty Cash\_QFS\_GL\_ACCOUNT\_ANALYSIS" worksheet, which listed the individual custodians, their college location, and the amount of cash in their care. We also reviewed the year end memorandums which document the cash count for each custodian and noted a difference of \$2,242. We met with Kyoko Connelly, Senior Accountant, and Charlene Rios, Director of Accounting, and reviewed the variance in the petty cash/change funds. Charlene noted it was due to changes in offered cash services on the campus, and multiple locations were returning cash to HQ and either closing or only accepting card payments. Charlene confirmed the variance was due to the GL not being updated with current cash assignments, and that the College was working to update the system. We determined the reported petty cash was overstated by \$2,242.18. The college had not performed a year end reconciliation of the cash and was alerted to the variance in testing. We recommend the college update their system with corrected cash assignments, and perform a year end reconciliation. See issue here [[V: Seattle Colleges Complete and Timely Cash Reconciliations](#)].

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**High** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

# State of Washington

## J.2.PR.G - Community & Tech College Testing - Seattle

*Procedure Step:* Cash and Cash Equivalents - Testing

*Prepared By:* MRF, 10/9/2024

*Reviewed By:* RKM, 10/20/2024

### Purpose/Conclusion:

#### **Purpose:**

To determine whether reported cash and cash equivalents existed as of the end of the period.

#### **Conclusion:**

We determined the reported balances existed at fiscal year end, are on hand and in the name of the college, and agree to actual amounts in existence at the bank.

We noted petty cash was overstated by \$2,242.18. As this is below the floor, we will not take it to the AOM.

### Testing Strategy:

#### **SAO Policy Requirement: Confirming or Verifying Cash & Investment Balances**

Confirmations can either be blind or a positive confirmation. In a blind confirmation (sweep), the auditor requests information on all accounts the bank holds for the entity (by entity name and/or EIN). In a positive confirmation, the auditor lists accounts (or accounts and balances) per the entity and asks the bank to confirm that the information is correct.

Confirm cash and investment account balances with County Treasurer, bank and/or brokerage. Use the template confirmation form provided in the Store when needed.

Confirmations can be mailed to addresses listed on the Bank Confirmation Address List available on the Auditor Reference Guide. If the bank notifies you of a different address, please contact Team Audit Support to update the list.

Banks may confirm incorrect amounts either due to a simple mistake, use of a wrong confirmation date or incorrectly including or excluding accounts. The first step in resolving differences should be to check information against the entity's bank statements and then call the bank to specifically confirm any difference.

Confirming investments may involve physical inspection, confirmation with the issuer, confirmation with the custodian, confirmation of unsettled transactions with the broker/dealer, confirmation with the counterparty, and/or reading



## State of Washington

executed partnership or similar agreements. When confirming investments, ensure investments are held in the entity's name.

*If confirmations are not used*, auditors must at minimum verify balances to the County Treasurer, bank and/or brokerage statements. If this is done, the auditor should consider the risk that the statements were altered and should examine papers for indications of alteration.

The following is a list of **additional considerations** for testing the existence assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### Bank Reconciliations

If the auditor is comparing reconciled (confirmed) bank or county treasurer balances to the GL (rather than confirmed amounts within an expected variance due to reconciling items), the auditor should consider performing some or all of the following tests to verify the accuracy of the reconciliations. Note that testing the reconciliation will provide evidence of both the existence and completeness of cash and investment balances.

Trace (or compare summed) bank balances per statements to reconciliations.

Trace (or compare summed) book balances per reconciliations to the general ledger or financial statements.

*If a cash account is allocable to a particular fund, the balance in the general ledger should be recorded in the same fund.*

Scan the reconciliation for reasonableness. Look for unusual, unexpected or vaguely described reconciling items, lack of support or detail, very large reconciling items, very old reconciling items, and missing or extra elements that would indicate that the reconciliation was being performed incorrectly.

Foot the reconciliation for accuracy.

Trace deposits in transit to the subsequent month's bank statement, considering reasonableness of the in-transit period.

Trace outstanding checks to cash disbursement journal.

Check that any other reconciling items are valid and have been properly accounted for (ex: large debit or credit memos).

Check reconciliation against prior and/or subsequent reconciliations for reasonableness of amounts and items included and to trace reconciling items from the previous and/or subsequent period.

### Other Tests

Inquire whether any checks or deposits were being held at year end for budget, cash flow or other purposes.

Confirm investments purchased but not received as of year-end

Confirm investments sold but still held as of year-end

Confirm interest due or accrued but not yet received as of year-end

## State of Washington

Search for manual journal entries that debit (increase) cash. Consider testing if risk indicators are noted.

Review reconciliations of clearing and transmittal accounts.

See accountability steps for testing strategies related to petty cash and imprest funds, which are not expected to be material to the financial statements.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Outstanding Checks and Deposits in Transit** – Per TIS section 1100.08 (AICPA Technical Questions and Answers), outstanding checks should be reported as a reduction of cash and the amount of deposits in transit should be reported as cash. A check is considered outstanding from the time that it is out of the payor's control – when mailed or delivered to the payee – until the time it clears the bank. Cash should represent amounts within the control of the reporting entity, that is, the amount of cash in banks plus cash and checks on hand and deposits in transit minus the amount of outstanding checks.

**SAO Audit Policy [6350](#) – External Confirmations**

### **Investments Area Guide**

Record of Work Done:

### **Significant Balances and Assertions:**

Higher Education Special Revenue Fund - Cash and Cash Equivalents - Existence

Higher Education Student Services Fund - Cash and Cash Equivalents - Existence

Controls are documented in the "Cash and Cash Equivalents - Controls" step.

### **Substantive tests performed to meet the Existence assertion:**

**See testing at** [\[Cash & Investments\]](#). Kyoko Connelly, Senior Accountant, provided us with the June 30, 2024 month-end reconciliation, BOA and US Bank investment/account statements, petty cash spreadsheet GL report and verification memorandums, to verify existence of cash and pooled investments as of 6/30/2024.

# State of Washington

## **Bank and Investment Statements**

We verified the existence of cash in the bank by reviewing the account statements for the Bank of America (main account), US Bank account (investment proceeds), and the LGIP account. We noted no issues.

## **Deposits in Transit**

We verified the existence of the deposits in transit by obtaining the "JUNE DIT" listing within the month end reconciliation. As there were 121 items, we judgementally selected 20 large deposits with different deposit types, which covered 68% of the amount, and traced them to a deposit on the July BOA statement.

There is a timing difference between what ctclink captures as a day's payment vs what the bank captures. As a result, the deposit amounts on the bank are slightly smaller than the deposit amounts on the DIT listing because subpayments are totalled differently. We received the "CC Merchant - June 2024" excel document and additional screenshots of deposit slips from Kyoko Connelly to tie the amount reported on the DIT list, to a deposit with the bank. The deposits tied with no exceptions.

## **Outstanding Checks**

We verified the existence of the outstanding checks by obtaining a list of all checks outstanding as of June 30th, 2024. We used the FS sampling spreadsheet and determined we needed to trace 37 checks for a high level of assurance.

We haphazardly selected 37 checks and traced them either to a deposit on the July BOA account, or the July 31st outstanding check report as generated by the bank. All tested checks tied with no issues.

## **Petty Cash/Change Funds**

Kyoko provided the "Petty Cash\_QFS\_GL\_Account\_Analysis" spreadsheet which listed each of the cash holding locations per the GL, and the year-end cash confirmation memorandums for each custodian and the amount verified.

We compared the amount of petty cash/change funds on the GL, the amount of cash that was physically verified at year end, and noted a difference of \$2,242.

We met with Kyoko Connelly, Senior Accountant, and Charlene Rios, Director of Accounting, and reviewed the variance in the petty cash/change funds. Charlene noted it was due to changes in offered cash services on the campus, and multiple locations were returning cash to HQ and either closing or only accepting card payments. Charlene confirmed the variance was due to the GL not being updated with current cash assignments, and that the College was working to update the system. We determined the reported petty cash was overstated by \$2,242.18. As this is below the floor, we will not take it to the AOM.

## **Comparison:**

We compared our verified cash balance as of June 30th, 2024, to the College's end of June reconciliation. While the college did note, and adjust, almost \$300k in "reconciling items" the College performed a complete year end reconciliation of cash balances. The only variance was due to the petty cash overstatement and was below the floor. We will not take this to the AOM.

## **J.2.PR.G - Community & Tech College Testing - Seattle**

# State of Washington

**Procedure Step:** Depreciable Capital Assets - Controls

**Prepared By:** EZM, 10/7/2024

**Reviewed By:** RKM, 10/8/2024

## Purpose/Conclusion.

### **Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

### **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy.

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

### **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

# State of Washington

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

## **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

## **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

## State of Washington

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria.*
---------------------

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:
----------------------

## **Significant Balance and Assertions:**

Internal controls in the Community and Technical College System address the following balance:

Governmental Activities - Depreciable Assets (Net of Accumulated Depreciation) - Existence, Valuation

See lead sheet here: [[Lead Sheet](#)].

## **STEP 1: Gain an Understanding of Internal Controls**

We met with the following individuals on September 11, 2024, to discuss controls over depreciable assets:

Terri Plischke, ctcLink Finance Pillar Lead (Finance Systems Specialist)

Kyoko Connolly, Senior Accountant – G/L

Michelle Nguyen, Senior Financial Analyst,

Miguel Gatmaytan, Purchasing Manager

Charlene Rios, Director of Accounting

David Williams, Director of Financial Reporting

## **Additions:**

### **Equipment/Library Resources**

Equipment/library resources go through the standard purchase requisition process. The process begins with the normal purchase order process that is used for all purchases. In addition to this, the requestor will fill out a fixed asset reporting (FAR) form with the equipment information including PO number, PO date, state tag, equipment description, and commodity code. Once the asset is confirmed as having been received, the equipment acquisition section of the asset reporting form will be filled out by the requester with the date received, custodian name, and asset location. This form is provided to Miguel Gatmaytan, Purchasing Manager, or Michelle Nguyen, Senior Financial Analyst, who will add the asset into the Asset Management Module (AM) in ctcLink using the invoice for asset cost. They review all information on the form for accuracy to ensure

## State of Washington

it has the correct commodity code (**Key Control 1 - Equipment Additions**). When an asset is added to the AM module, the entry also automatically results in a General Ledger Journal that is reviewed by accounting staff and posted to the GL.

### Buildings and Improvements

Buildings and improvements are funded through COP and are usually multi-year budgeted projects. During the construction, Project Managers from each campus approve construction invoices, alongside DES, department capital teams, and VP Administrators, and forward them to Michelle for processing. At the end of the year, Michelle runs a query to pull capitalized building expense accounts to review the expenditures. When a building project is completed, the totality of the relevant expenditures will be capitalized from construction-in-process via a journal entry and buildings still under construction will have expenditures added to CIP in ctcLink.

### Depreciation

The College relies on ctcLink's calculations for depreciation expense. ctcLink automatically calculates an asset's depreciation based upon manual input of a commodity code (provides service life), the cost of the asset, and in-service date (**Key Control 2 - ctcLink Depreciation Calculation**). Miguel manually inputs this information into the Asset Management module and then Terri Plischke, ctcLink Finance Pillar Lead (Finance Systems Specialist), compares Manuel's entry in the AM module to the FAR form to ensure that the commodity code and in-service date are accurate. The service dates uses either the occupied date for buildings or investment date for equipment/resources. The calculation is performed monthly – Terri manually runs the automatic depreciation calculation for all depreciable assets once a month.

### Disposals

Disposals are initiated via a request from campus departments to purchasing, after approval from the department. Assets can either be repurposed for use throughout the college or surplus through DES. Miguel handles DES surplus and submits a request with a listing of assets being sent for surplus. The request is approved by DES and the college is sent a Surplus Authority number. Once the assets are sent and the surplus authority is fulfilled, Miguel will remove the assets from ctcLink. (**Key Control 3 - Depreciable Capital Asset Removals**) Michelle is responsible for removing building assets when a building is demolished. She works with the college and SBCTC or DES when necessary. Library resources are also removed from ctcLink by Michelle when they are fully depreciated.

### Inventory

Per Miguel Gatmaytan, the College performs a physical inventory every two years, broken into two rounds. The first round will have Miguel and custodians identify as many of the assets as they can for District, Central, North, and South campuses. The second round consists of Miguel attempting to locate all assets that were not found during the 1st round. Miguel stated that they have completed the first round for FY2024-25 back in Spring 2024 and they're about to start the second round, starting with the North campus, in Fall 2024. and expect to complete the first round for all campuses by January 2024.

### GL to AM Reconciliation

According to Terri Plischke, during the fiscal year, two reconciliations were performed between the general ledger and the Asset Management



## State of Washington

module. She explained that they did one early in the fiscal year and they did one close to fiscal year end. They could not, however, provide us with any documentation showing who performed/reviewed this reconciliation, or when the reconciliation occurred. When we performed our own comparison between the GL and AM module during testing, we found that the variance between the two was insignificant and below the floor.

### Key Controls:

**Key Control 1: Equipment/Library additions are recorded in ctcLink from invoices and fixed asset reporting forms (Existence, Valuation).**

**Key Control 2: ctcLink automatically calculates an asset's depreciation based upon manual input of a commodity code (provides service life) and in-service date (Valuation).**

**Key Control 3: Depreciable capital asset disposals are initiated via a request from campus departments. The Purchasing Manager submits a surplus request with a listing of assets being sent for surplus to DES, who will then approve the request. Once that request is fulfilled, the Purchasing Manager then removes the assets from ctcLink.**

### Identified Weaknesses:

None.

## **STEP 2: Confirm Key Controls**

**Key Control 1: Equipment/Library additions are recorded in ctcLink from invoices and fixed asset reporting forms (Existence, Valuation).**

We reviewed invoice #75183 sent October 13, 2023 in the amount of \$67,576.64 and the fixed asset reporting forms (FARF) associated with the invoice recording asset 1000205. We noted that the total of \$67,576.64 was for the purchase of 3 separate medical equipment items - one of these items was the Pyxis MedStation ES Main 6 Drawer. We found that the total cost of this item on the invoice tied to the cost amount in ctcLink Asset Management (AM) module and to the FARF without exception. **No issues noted**

**Key Control 2: ctcLink automatically calculates an asset's depreciation based upon manual input of a commodity code (provides service life), the cost of the asset and in-service date (Valuation).**

See confirmation of the automated control at [[IT Control Testing - Depreciation](#)]. **No issues noted.**

**Key Control 3: Depreciable capital asset disposals are initiated via a request from campus departments. The Purchasing Manager submits a surplus request with a listing of assets being sent for surplus to DES, who will then approve the request. Once that request is fulfilled, the Purchasing Manager then removes the assets from ctcLink.**

We inspected a surplus request form for asset #734327, a microfilm reader from the South campus's library. The surplus request form was submitted on 8/17/23 by Seattle Colleges staff, was approved by DES, and was then later removed from the asset listing by Miguel Gatmaytan, Purchasing Manager. We confirmed this by reviewing the asset master log from FY24, and we noted that the asset had a disposal date of 8/18/23, after the surplus request was submitted. We also inspected the "QFS\_AM\_ASSET\_COST" query we received from David Williams,

## State of Washington

Director of Financial Reporting, which listed all of the assets currently in the custody of Seattle Colleegs, and we noted that this asset was not included in the listing, further evidencing that it was properly disposed of. **No issues noted.**

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

#### **J.2.PR.G - Community & Tech College Testing - Seattle**

*Procedure Step:* IT Control Testing - Depreciation

*Prepared By:* EZM, 10/7/2024

*Reviewed By:* RKM, 10/8/2024

Purpose/Conclusion.
---------------------

#### **Purpose:**

To determine whether the automated control was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently

# State of Washington

during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [Depreciable Capital Assets - Controls].

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the*

## State of Washington

*entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

## State of Washington

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

## State of Washington

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

## Information Technology Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

### **STEP 1: Understand Automated Key Control**

**Significant System:** ctcLink - Asset Management module

**Key Automated Control:** ctcLink automatically calculates an asset's depreciation based upon manual input of a commodity code (provides service life), the cost of the asset and in-service date.

Our understanding of the overall control is documented as part of our understanding of controls over relevant assertions for Asset Management in the "Depreciable Capital Assets - Controls" step.

### **STEP 2: Confirm and Test Automated Key Control:**

We confirmed and tested the key automated control as follows, to determine whether the software calculation correctly valued each transaction:

We tested the same assets selected in our valuation/existence sample. We used a 7.5% tolerable misstatement and a low assurance to select and recalculate accumulated depreciation on 6 asset additions (and 6 reductions only to determine removal of asset to zero value) to confirm the automated control and determine whether the software correctly valued each transaction. We used a report from Asset Management (AM) called

## State of Washington

"Asset Master Log" showing the fields included in the calculation. The fields used in the calculation are useful life, salvage value, asset cost, and in-service date. We then recalculated the accumulated depreciation and tied the amount back to the amount actually posted in AM. See testing at [Depreciable Capital Assets]. We determined that the system is accurately calculating monthly depreciation based on the date entered for sampled items. **This automated control is in place.**

### **STEP 3: Understand General IT Controls**

The following people have access to the Asset Management module in ctcLink (**Key Control 1 - User Access**):

- Terri Plischke, ctcLink Finance Pillar Lead (Finance Systems Specialist)
- Kyoko Connolly, Senior Accountant – G/L
- Michelle Nguyen, Senior Financial Analyst,
- Miguel Gatmaytan, Purchasing Manager
- Charlene Rios, Director of Accounting
- David Williams, Director of Financial Reporting

Terri informed us, however, that only Miguel and her actually use the system – the other individuals who have access, who were present in the meeting, expressed that they were unable to navigate the system due to its complexity.

David informed us that Seattle Colleges staff were unable to make changes to how the system calculates depreciation. He further explained that college staff that are given access to the module are only able to enter information (such as asset cost, commodity code, and the in-service date) into the system - they cannot change how the system operates. He explained that SBCTC and Oracle, who is the vendor for ctcLink, would work in conjunction with one another to make changes such as that to the system.

If the College identifies an error with how the system operates, College staff would submit a ticket with SBCTC to determine the cause, and SBCTC would then work with the appropriate IT professionals to resolve the issue. If College staff found an error with the data inputs (commodity code, in-service date, total cost, etc.), they have the ability to adjust that in AM by adjusting the record. This would result in both an adjustment to the record in AM and an automatically generated correcting journal entry that would be reviewed and posted to the GL. College staff informed us that they could not recall any errors with how the system operating during FY24.

### **STEP 4: Confirm Key General IT Controls**

**Key Control #1 (User Access) - Only certain individuals have access to the Asset Management module.**

We received a spreadsheet titled "AM.Module.Roles.2024" which listed all of the Seattle Colleges staff members that had access to the Asset Management module, as well as what roles each member was assigned. We reviewed the spreadsheet and confirmed that only the following individuals had access to the Asset Management module:

- Terri Plischke
- Kyoko Connolly
- Michelle Nguyen
- David Williams



# State of Washington

Miguel Gatmaytan  
Charlene Rios

***No issues noted.***

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

## **J.2.PR.G - Community & Tech College Testing - Seattle**

***Procedure Step:*** Depreciable Capital Assets - Testing

***Prepared By:*** EZM, 10/9/2024

***Reviewed By:*** RKM, 10/10/2024

Purpose/Conclusion:

### **Purpose:**

To determine whether reported capital assets represent real assets, as of the end of the period (Existence).  
To determine whether capital assets are reported at properly valued and calculated amounts (Valuation).

### **Conclusion:**

We determined that reported capital assets represent real assets, as of the end of the period (Existence).  
We determined that capital assets are reported at properly valued and calculated amounts (Valuation).

Testing Strategy:

The following is a list of **considerations** for testing the existence assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Nonexistent Assets**

## State of Washington

Review capital asset records to determine whether records meet minimum requirements of BARS [3.3.9.40](#) to positively identify and adequately describe the asset. If asset records are not sufficient, follow up on how the entity is able to identify and track reported assets and consider further audit procedures.

Scan the capital asset list for unusual or unexpected assets or patterns.

*For example: asset descriptions that appear insufficient to identify the asset, asset descriptions that seem strange, assets with a historical cost that doesn't appear to meet the capital asset threshold, assets that are past the end of their service life, assets or asset types that don't appear to belong (based on auditor's understanding of entity activities and area of operation), assets or asset types that the auditor doesn't recognize, attributes that appear unreasonable (historical cost, useful life or scrap value), assets that appear connected to actions noted in planning procedures (impairment, replacement, sale or surplus, transfer), etc.*

Test sampled assets or selected high-risk assets from accounting records for existence by observing them or reviewing documentation.

*Observation for aboveground infrastructure such as roads, bridges or buildings may be by [google maps](#). Documentation for underground assets may consist of maps, system plans approved by regulatory agencies or permits, etc.*

Review the government's records of the latest physical inventory for any identification and follow-up on missing assets or any types of assets or locations that were not covered. Note: review of a government's physical inventory is considered a control test. However, it may be done as a risk assessment procedure to help direct substantive testing, and follow-up on results may result in some substantive evidence.

Trace assets from accounting records to assets listed on the government's insurance policy records. Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

Trace assets from accounting records to operational records (ex: Public Works Department typically tracks assets for maintenance or regulatory reporting purposes). Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

For land and buildings, trace parcels and historical cost per the land subsidiary schedules to the County's land (GIS) records to verify ownership. Note: this test also provides evidence for the rights & obligations assertion and - if a complete list is obtained from the County - for the completeness assertion as well.

Compare reported public project completed or in process during the period to the L&I [prevailing wage reporting database](#). Note: since reporting is done by contractors, it would be considered a third-party verification of project existence. We would expect capitalized costs (which include costs incurred by the government as well as contractors) to exceed the contractor's reported costs for most projects. This test also provides evidence for the completeness assertion if traced from the L&I database.

### **Cut-off**

Review supporting documentation to verify dates of any transfers, annexations or donations.

# State of Washington

See the Expenditures | Existence step for testing strategies on cut-off for capitalized expenditures.

## Detail Roll-Up

If manual journal entries are required to update the GL, agree figures per the GL to subsidiary schedules or systems.

Search for manual journal entries that debit (increase) capital or infrastructure assets. Consider testing if any risk indicators are noted.

Reconcile (or review the government's reconciliation) capital expenditures for governmental funds to increases in capital assets. The only anticipated reconciling item would be equipment that is below the capitalization threshold.

Reconcile (or review the government's reconciliation) increases in capital assets to capital purchases and sales per the statement of cash flows for proprietary funds. The only anticipated reconciling item would be donated or contributed assets.

**Over/Invalid Capitalization** - See classification step for testing strategies on improper capitalization upon construction or acquisition, or when determining whether an expense is a maintenance or repair expense or a capitalized improvement.

## Unrecorded Disposals or Impairments

Scan capital asset records for fully depreciated assets and inquire as to the status (disposed, no longer in use, etc.) to ensure all retirements and disposals have been recorded. Evaluate appropriate accounting for any fully depreciated assets remaining in service in accordance with [BARS 3.3.10.130](#).

Identify significant disposals, impairments (due to obsolescence or damage) or contributions per review of minutes and trace to asset records to verify these events were accounted for.

Request a list of insurance claims made during the audit period to identify possible impairments or removed assets, then trace to subsidiary records to verify that the event was properly accounted for.

Identify annexations (through minutes, inquiry or OFM's central annexation tracking system) and trace to supporting documents showing the transfer of assets. Note: this test would also provide evidence for the completeness and rights & obligations assertions.

The following is a list of **considerations** for testing the valuation assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## Incorrect Depreciation Calculations

Perform an analytical review of depreciation expense by type of asset for reasonableness.

Re-calculate depreciation expense for a sample of assets or in conjunction with a test of automated controls (if depreciation is automatically calculated by the system). Consider testing the inputs used for the calculation to determine whether they are reasonable and in line with any applicable policies; i.e. useful life, salvage value, etc. Alternatively, test calculations, extensions and footing of subsidiary records if records are maintained on spreadsheets.

Evaluate capital asset policies for componentization or grouping of assets to determine if it has been consistently followed and will result in a rational method of depreciation. See BARS [3.3.10.150](#) for guidance.

## State of Washington

Evaluate estimated useful life and scrap value factors for reasonableness. This test could be done in general (on the government's accounting policies), for selected asset classes or for selected or sampled asset records.

*If testing selected high risk assets, auditors should consider assets that are nearly or fully depreciated (see BARS [3.3.10.130](#)), assets with unusually high or low useful lives for their type, and assets with unusually high scrap values.*

Compare estimated useful lives for assets with replacement schedules / policies and capital budgets.

*We would expect that assets on a regular replacement schedule (such as equipment, vehicles, road surfacing, etc) or that are included for replacement in the capital budget would have estimated useful lives that match the government's replacement plans for the asset.*

Consider whether the date placed in service for assets is reasonable given when the asset begins being used or is substantially complete as this will have an effect on when depreciation begins. See information in BARS [3.3.10.90](#) about when to move a project out of CIP.

### **Impairment**

Check that the measurement method used for write-offs is in accordance with GAAP (GASB 42.12-15). Review or recalculate the portion of historical cost that should be written off for impaired capital assets. *Note: auditor would normally use the same measurement method used by the government unless it the auditor finds it inappropriate for the circumstances or unallowable under GAAP.*

### **Incorrect Historical Cost of Assets**

Trace recorded cost to supporting documentation. *Note: This test would normally be limited to recent additions, since documentation for historical assets has likely passed the records retention period.*

Evaluate the reasonableness of any estimates of the historical cost of capital assets.

Evaluate the reasonableness and support for any estimates of the acquisition value (per GASB 72) of donated capital assets.

### **Conversion to GAAP**

For governments converting to GAAP reporting, examine valuation method for retroactively reported infrastructure assets and verify that the valuation method used is one of the methods prescribed by the County Road Advisory Board.

### **Modified Approach**

Check that infrastructure is being depreciated unless the modified approach is used. If the modified approach is used, verify that the government has met criteria of GASB 34 par 23-26.

### **Allocation**

On the government-wide statement of activities, review allocation of depreciation for capital assets for governmental funds. Depreciation expense

## State of Washington

will be reported as a component of the direct expense shown in the statement of activities. Request spreadsheet for allocation.

Guidance/Criteria:

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

GAAP criteria for reporting capital assets

[\*\*GASB Codification Section 1400 Reporting Capital Assets\*\*](#)

[\*\*GASB Comprehensive Implementation Guide Chapter 7 Basic Financial Statements and Management's Discussion and Analysis, sections 7.9-7.21\*\*](#)

Record of Work Done:

### **Significant Balance and Assertions:**

Governmental Activities - Depreciable Assets (Net of Accumulated Depreciation) - Existence, Valuation

Controls are documented in the "Depreciable Capital Assets - Controls" step.

### **Substantive tests performed to meet the Existence assertion:**

We used the small population sampling spreadsheet (7.5% tolerable misstatement, low assurance) to determine our sample size. We haphazardly selected 6 additions and 6 disposals for testing.

### **Additions & Reductions Testing:**

We tested for the following attributes related to **Existence**:

A = The asset meets OFM capitalization criteria (SAAM 30.20)

B = Acquisition date/disposal date was properly recorded, traced to invoice/disposal form and amount reported represents actual costs that exist of as of the report date.

See testing at: [[Depreciable Capital Assets](#)] tab "3 - Existence Valuation". For selected assets, we obtained invoices, fixed asset reporting forms, purchase orders, disposal requests and email documentation from David Williams, Director of Financial Reporting.

Our additions and reductions testing did not note any issues related to existence. **No issues noted.**

### **Substantive tests performed to meet the Valuation assertion:**

# State of Washington

See above for sampling methodology.

## Additions & Reductions Testing:

We tested for the following attributes related to **Valuation**:

C = The asset is recorded at historical cost as compared to original invoice and all ancillary charges necessary to place in intended location or Asset is properly removed from asset listing, equaling zero value at year end.

D = **IT CONTROL** - ctclink automatically calculates straight-line depreciation based on asset information entered: in-service date, commodity code, and asset value.

See testing at: [[Depreciable Capital Assets](#)] tab "3 - Existence Valuation". See attribute E - IT Control Testing Depreciation ROWD here: [[IT Control Testing - Depreciation](#)].

Our additions and reductions testing did not note any issues related to valuation. **No issues noted.**

## J.2.PRG - Community & Tech College Testing - Seattle

*Procedure Step:* Charges for Services - Controls

*Prepared By:* MRF, 9/17/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion.

### **Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

### **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

# State of Washington

Testing Strategy:

**This workbook template was designed for tuition revenue system control audits at Community Colleges. Contact [Team IT Audit](#) with questions on information or steps contained in this template. The template assumes occurrence and valuation are relevant assertions and that controls over occurrence and valuation will be tested.**

The following procedures are **required** for all relevant systems:

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption [RCW 42.56.420](#) for cyber security purposes. The details documented in the record of work and supporting workpapers may qualify for this exemption. Auditors must include this statement in workpapers: "**This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited**".

## **STEP 1: Control Understanding**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*See the **Client Resource Tab** to reference query tools and year end adjustment information applicable to community and technical colleges. The following are expected controls for and community technical colleges. If sufficient key controls are not in place, the government may be able to demonstrate compensating controls.*

*Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of COSO elements as documented in the "Entity-wide COSO Evaluation" step as they relate to this particular system.*

When gaining an understanding of a college's tuition revenue system, the following specific steps should be considered:

### Admissions & Class Registration

Discuss admissions and class registration procedures with department representatives or registrars to gain an understanding of admissions and registration processes and policies. Consider the following:

How is a student's status validated?

How do they assure that a student's status has been accurately posted from Campus Solutions Core to Student Finance (SF)?

# State of Washington

## Tuition calculation

The automated tuition calculation processed in the cTcLink system has been identified as an automated control. When gaining an understanding of a college's software calculation controls, the following specific steps should be considered:

Gain an understanding of the college's procedures for updating Term Fees, Tuition Groups, Item Types, and Tuition Schedule tables, including any review they perform to ensure the changes made are correct.

Validation of Tuition Calculation at the College - Inquire with college staff to see if they test tuition calculations prior to rolling over term fees, and if so, whether they used the Production College Development (PCD) environment to do so. If they have saved supporting documentation for testing performed, observe testing results to verify that the respective tuition and fee values were actually calculated correctly for each category of mock student tested.

Identify individuals responsible for updating the tuition rates including any users who are authorized to modify the tables or access the screens which have been deemed critical to the tuition revenue calculation process (Term Fees, Tuition Groups, Tuition Calculation, Item Types, and Tuition Schedule)

Consider obtaining the following from college staff when testing calculation of tuition revenue for a sample students:

Approved tuition rates

**Customer Account** reports showing tuition/fee charges on the student accounts

**Customer Academic Information** and **Career Term** data showing the student's status/tuition group

**Enrollment Summary** showing evidence of the classes the student was enrolled in for the selected quarter.

## Tuition payment

Students typically pay tuition and fees by credit card. Credit cards are processed through CyberSource. State and community technical colleges must reconcile payments received, and each individual college establishes their own frequency to complete it. Each cashier closes out daily using a batch report from the cTcLink system. The daily batch report may not include daily transactions for EFT's and wires. The following steps should be considered when gaining an understanding of tuition payment:

Discuss cash receipting procedures with department staff and document procedures performed tuition payments paid with the following

Cash or check

Credit Card

ACH/Wire

We expect colleges reconcile credit card payments made through CyberSource. Inquire and document the colleges process of tying credit card payments processed through CyberSource to entries made in the cTcLink system.

Inquire regarding how the college would address variances found when performing reconciliations.



# State of Washington

## Posting to the GL

Receipts are posted to the GL through an evening automated batch process. Typically, cash receipts are reconciled daily to bank accounts, and bank account balances reconciled monthly to cTcLink. Consider the following:

Gain an understanding of the GL posting process, and determine how they validate that their postings are accurate and complete.

Inquire regarding how the college would know if the GL did not post accurately or completely. It is likely there will be variances in how each college performs their reconciliations, with some using spreadsheets or running queries or customized reports as tools to validate the GL postings.

## Distribution / Allocation to Revenue accounts

Review the procedures the college uses to assure that all tuition revenue payments from GL fund 840 were completely distributed. Consider the following:

Document the process used by the colleges to update/maintain the values in their Tuition Distribution table.

## Transfer to AFRS

Gain an understanding the college's reconciliation process of their cTcLink balances to those posted to AFRS. Consider the following:

Evaluate the college's procedures regarding the year-end closing entries recommended by the State Board (per their "Year End Closing" binder). While the key control is the reconciliation done by the SBCTC, the college still needs to provide oversight and monitoring of the adjustments that are recommended by the SBCTC (colleges should understand what the adjustments are for, that they are correct and properly supported).

*Note:* SBCTC System Accounting Coordinators handle all ctcLink uploads to AFRS. Every month, on AFRS cutoff date, a staff from SBCTC runs a query in ctcLink of all journal entries created. This is a summary level report that is downloaded into an Excel spreadsheet. Staff create two pivot tables; one by funds and amounts, another by general ledgers and amounts. Staff expects the pivot table by fund and amount to be zero. Staff then compares the second pivot table to another report, which is generated for the State Auditor's Office (SAO). Both reports are queried from the same database, the one for SAO contains a few more fields. When all the amounts agree, staff is ready to prepare the file to be uploaded into AFRS.

Staff then sort the file by fund, general ledger, and amount. The customization now generates the output files (flat files with transaction codes) and sends them to AFRS. There are usually 1600 to 2200 lines for each college each month. This file is saved as a flat file format and is uploaded into AFRS using the OFM's Financial Toolbox. Sue does a test run in what is known as the SUP environment (copy of previous day's production) to check for any major issues. Staff is able to capture a copy of the flat file and uses that to reconcile between what is in ctcLink and what was transmitted to AFRS. Staff makes any necessary corrections to the AFRS batch and releases the output file to AFRS.

# State of Washington

Financial Adjusting Entries – the colleges are directed to use the adjusting entry forms to enter any required cTcLink adjustments, with each suggested adjusting entry denoted in this section. Additional explanations (from the SMARTER system) for each of the suggested adjusting entries are also provided.

SMARTER Queries used to reconcile Finance Sub Modules to the General Ledger. Not all State community and technical colleges use SMARTER Queries, however, use is encouraged by SBCTC.

*Note: Waivers are not included in data reported from cTcLink to AFRS*

Disclosure Forms – Copies of the college's general note disclosures and supporting documentation.

Payable/Receivable reporting reflecting any payables ("due to") and receivable ("due from") transactions with other state agencies.

*Note: Some reports and queries used by colleges may be built in-house and may be used alongside SMARTER queries that have been built by SBCTC. If the college does not have a good understanding of the reconciliation process done by the SBCTC then the auditor may want to consider reviewing the year-end adjustments for material errors. For example, the auditor could request the Year End Closing documentation from the State community or technical college and review it to determine the types of adjusting entries and exception items noted by SBCTC.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

## **Step 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4.A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.*

## **STEP 4: Test Controls**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted,*

## State of Washington

*auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

***Since key controls for Tuition Revenue are automated, Auditors should add the "IT Control Testing - Tuition Calculation" step available in the Store to document automated and general control testing.***

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of COSO elements. In doing so, all of the following specific determinations must be documented:*

- A. Key controls – including personnel who affect the application of the control – have not changed since they were last tested. Automated controls should be tested the first year that colleges use the cTclink system.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2021, this work could potentially be relied upon for both the periods ending 2022 and 2023.*

### **Step 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

## **SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

### **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Education - Higher Education Charges for Services - Occurrence, Valuation  
Higher Education Special Revenue - Charges for Services - Occurrence, Valuation

See lead sheet here: [\[Lead Sheet\]](#)

### **STEP 1: Gain an Understanding of Internal Controls**

Software used by community colleges to generate tuition revenue is developed and maintained by State Board of Community and Technical Colleges (SBCTC). Student information is captured in the ctcLink system in Campus Solutions Core module. Tuition is automatically calculated and applied to student accounts within Student Financials (SF). The rates and codes used in the tuition calculation process reside within several key system tables, which are maintained in part by SBCTC and by the local colleges.

Seattle Colleges is actually a group of three colleges, each with their own business unit; WA062, WA 063, and WA064. When the three colleges have their data combined and posted to ctcLink, it is under the business unit WA060.

### **Admissions & Class Registration**

Students can register on-line at the Admissions office. Critical information associated with tuition revenue is captured at this point regarding the student's status (i.e. resident, non-resident, veteran, etc.), and this data is posted to the Campus Solutions Core module.

The Admissions office processes the student applications within Campus Solutions module. When the first billing record is generated for the student (i.e., for admissions or testing fees), an account is created for the student in the Campus Solutions Core module.

Students typically register for classes on-line, but they can also do so in person. Classes are defined within the Campus Solutions Core module. The information captured in Campus Solutions Core during registration will be used in calculating the amount of tuition owed by each student.

## State of Washington

A student's tuition and fee liability is recorded in the Campus Solutions Core database when students register for classes, but revenue will not be recognized in the GL until a journal is created in Campus Solutions Core and sent to Student Financials via nightly batch.

At the time of the student enrollment, the Campus Solution module generates the student's class schedule which calculates the tuition and fees to the student's account based on a student's enrollment information (i.e. classes, hours), residency status, and any applicable tuition waivers. An individual student may be enrolled in two different colleges simultaneously.

### Waivers - Admissions Office and Registration

There are three types of waivers:

- Residency Classification – This waiver allows individuals to pay in-state tuition even if they have not resided in Washington State for the prior 12 months (i.e., Active Duty Military and Dependents)
- Mandatory Classification – These waivers are mandatory by RCW or SBCTC policy (i.e., Children and Spouses of Deceased or Disabled Law Enforcement Officers or Firefighters)
- Optional Classification – Colleges have discretion in whether to participate in optional waiver programs and how much to waive (i.e., Athletic waivers, running start).

The College uses all of the SBCTC waivers but has waivers unique to the College. The waivers are created in the PCD environment (testing) in ctcLink. After verifying they have been entered correcting they will be released/input into PRD (production).

### Tuition Calculation

The Campus Solutions (ctcLink) automatically calculates student tuition and fee charges from the student account, student course registration, tuition and fees entered (**Key Control 1 – Automated ctcLink Valuation**). The report will run for students that have made any changes in schedules every day and every week for all students. However, a known weakness exists in ctcLink. The system makes revenue and accounts receivable entries as soon as a student registers. This is incorrect as there has been no exchange of value and the colleges do not have yet a legally enforceable claim on those resources. SBCTC communicated this matter to colleges in a memorandum along with instructions on how to prepare a correcting journal entry. This weakness is addressed by key control #3 noted below.

The tuition revenue calculation processing resides within a third-party vendor application system, which cannot be modified by system users. The only way for college users to affect the calculation is through edits to associated data tables and screens and many of those tables are restricted to modification by State Board at the college level.

### Term Rollover and Tuition Updates

The calculation of student tuition and fees is automated in the ctcLink system based on rate tables and student's demographic information and course load. Our understanding of the automated control is documented as part of our "IT Control Testing" program step. We performed testing of this automated calculation at the IT Control Testing step here [IT Control Testing - Charges for Services].

# State of Washington

## **Tuition payment**

Tuition can be paid on-line, by phone, or in person at the Cashier's office. Payments are captured by the Campus Solutions subledger for ctcLink. This will only hit the GL once a week when they close out the cashiering job. ctcLink generates the files and sends them to the college once a week. Revenue is posted to the GL after the payment is received, the account receivable for the student's tuition is also reversed at the time of payment.

Cashiers receive payments and code receipts by student, which automatically hard codes to fee codes set in the system. The speed type have all coding information that will go to the GL codes. Students can either pay at the office, mail, or at the cashier's office that is collected and entered in the ctcLink system by Cashiers. Payments must be received prior to the posted tuition deadline. If payment is not received the student is dropped. Depending on the timeframe of the deadline they will get 100%, 50%, or no refund. Registration staff identifies dropped students and gives cashiering a dropped students listing.

Cashiers at each College reconcile their drawers each day. The deposits are picked up daily and delivered to the bank. A deposit slip goes with the actual bank deposit and is sent to the Accounting Office. The Accounting Office uses the deposit slips to ensure the information in the bank account is accurate. Bank statements are reconciled to GL activity each month by an Accountant and reviewed to ensure reported revenue activity agrees to the bank statements **(Key Control 2 - Occurrence)**. See cash & pooled investment controls at: [\[Cash and Cash Equivalents - Controls\]](#)

## **Posting to the GL**

Tuition revenue is recognized when a student's enrollment is complete and student status is validated. Upon completion of the student's enrollment, a journal entry is created in Campus Solutions Core and sent to Finance via nightly an automated nightly batch process.

Cash receipts are posted to the GL through a nightly batch process, and if there are posting problems, the system notifies the user that the batch did not post. Corrections are made through a batch edit screen, and the corrected batch is remitted. Tuition payments result in revenue being posted to Fund 840 under the source codes 0424 (tuition) and 0430 & 0431 (supplemental fees). Note that Spring/Summer pre-payments for Fall Quarter tuition are posted to GL account 5192 (deferred revenue).

To ensure only the revenues that occurred during the fiscal year are recorded, the College reviews unearned tuition revenue reports. This report shows them the amount that is unavailable revenues. After fiscal year-end, the unearned tuition revenue report is reviewed for the amount of unearned revenue and the report is used as support for the for the adjustment to move tuition from GL account 2040010 to the correct fiscal year related to when the services will be provided and the revenue earned/recognized **(Key Control 3 - Occurrence)**.

## **Distribution / Allocation to Revenue accounts**

An automated monthly process is run in ctcLink to allocate tuition revenue payments from GL fund 840 to the funds below. With the exception of Service & Activities fees (set by the Local Board of Trustees), the individual fund distribution percentages are determined by the Legislature. The local college manually posts and retains these percentages in the Tuition Schedule.

## State of Washington

060 (Building fee portion; remitted back to the State)  
149 (Operating fee portion)  
522 (Services & Activities portion)  
561 (Comm/Tech College Innovation portion)  
860 (Institutional Financial Aid portion)

An automated monthly process is run in ctcLink to allocate tuition revenue payments from GL fund 840 to the funds below. With the exception of Service & Activities fees (set by the Local Board of Trustees), the individual fund distribution percentages are determined by the Legislature. The local college manually posts and retains these percentages in the Tuition Schedule.

We obtained the tuition and fee schedule from Lee Grubb (FY24-ctc-tuition-and-fee-detail.pdf).

### **Transfer to AFRS**

The process continues to be a manual, although SBCTC is working on an automated interface to transfer financial data to AFRS. The System Accounting Coordinator handles all ctcLink uploads to AFRS. Every month, on the AFRS cutoff date, the Coordinator runs a query in ctcLink of all journal entries created. This is a summary level report that is downloaded into an Excel spreadsheet. The Coordinator then creates two pivot tables; one by funds and amounts, another by general ledgers and amounts. Staff expects the pivot table by fund and amount to be zero. Staff then compare the second pivot table to another report, which is generated for the State Auditor's Office (SAO). Both reports are queried from the same database, the one for SAO contains a few more fields. When all the amounts agree, staff prepare the file to be uploaded into AFRS.

Staff then sorts the file by fund, general ledger, and amount. The customization now generates the output files (flat files with transaction codes) and sends them to AFRS similar to how it is done in the Legacy system. There are usually 1600 to 2200 lines for each college each month. This file is saved as a flat file format and is uploaded into AFRS using the OFM's Financial Toolbox. A test run in what is known as the SUP environment (copy of previous day's production) is then used to check for any major issues. Staff is then able to capture a copy of the flat file and uses that to reconcile between what is in ctcLink and what was transmitted to AFRS. Staff makes any necessary corrections to the AFRS batch and releases the output file to AFRS.

ctcLink automatically posts to the Agency Financial Reporting System (AFRS) on a monthly basis. Colleges utilize a web-based tool called SMART (Standard Monthly Analysis and Review of Transactions) to identify transaction posting problems and make correcting entries in the college's accounting system. After ctcLink closes at year-end, they use SMART to enter adjustments which are posted to AFRS by the State Board (SBCTC).

SBCTC is responsible for the reconciliation between the ctcLink data to the AFRS data. The reconciliation is performed on a monthly basis and exception reports are produced that are researched and corrected. SBCTC sends the college monthly error reports that have to do with AFRS coding issues.

## State of Washington

At the end of the year when the College prepares their financial statements, they perform a *Tuition Waiver* calculation in compliance with NACUBO (National Association of College and University Business Officers) standards. SBCTC provides the template to the College as an excel workbook. David Williams, Director of Financial Reporting, fills in the various tabs of the calculator workbook with the financial data of the college as pulled from ctclink. The total "tuition waiver" is meant to represent the total amount of discounts provided to students throughout the year from both federal sources and state sources such as the College itself. Many of these discounts are monetary scholarships or fee waivers, but some discounts are non monetary and must be assigned an estimated value. The summary amounts of each type of waiver/discount is applied to the worksheet and the calculation page, which currently follows the "alternative method" of NACUBO advised in 2000. This amount will reduce the reported revenue from student tuition and fees on the financial statements. David noted that the annual amount of discount is related to the needs of the student population and will fluctuate from year to year, but estimated the typical amount to be between \$10-14M.

We followed up with David on 10/10/2024 and discussed how the adjustment is reported. David explained that the adjustment isn't performed until the year end financial statements are developed up to 15 months after fiscal year end. The financial statements are reported on a full accrual basis as opposed to the statewide modified accrual basis. As a result, this discount adjustment is not reported in the AFRS database and is not considered in the reported tuition revenue for higher education. We will follow up on this with OFM and SBCTC to determine if the allowance is included in the statement of activities.

### **Key Controls:**

**Key Control 1 – AUTOMATED (ctcLink) Valuation** - The College's ctcLink subledger, Campus Solutions, creates student's class schedules which then automatically calculates tuition and fees, based on student data, tuition codes, and tuition rates set up within the system to ensure tuition and fees due are properly calculated.

**Key Control 2 - (Occurrence)** - Bank statements are reconciled to GL activity each month by an Accountant and reviewed to ensure reported revenue activity for tuition payments agrees to the bank statements and general ledger.

**Key Control 3 - (Occurrence)** - After fiscal year-end, the unearned tuition revenue report is reviewed for the amount of unearned revenue and the report is used as support for the for the adjustment to move tuition from GL account 2040010 to the correct fiscal year related to when the services will be provided and the revenue earned/recognized.

### **STEP 2: Confirm Key Controls**

**Key Control #1- Automated (ctclink) Valuation** - We confirmed the automated key control at [[IT Control Testing - Charges for Services](#)].

**Key Control 2 - (Occurrence)** - We reviewed the June 2024 month end reconciliation of the student financials module to the general ledger to ensure amounts collected were correctly posted. Lee Grubb (Assistant Director of Student Financials) provided us with the "June 2024 SF to GL.xlsx" spreadsheet which detailed all transactions reconciled for the month of June. The "GL data" tab listed each transaction through the month, the amounts, the accounts and a description/coding of the revenue/expense type. The "combined" tab was all three college's student financials data combined into one listing. The "Analysis" tab imported the data from the other two tabs in a pivot table and sub totaled each



## State of Washington

account by fund and comparing the SF to the GL. We noted the column which calculated the variance between the two had occasional small amounts of variance and each variance had a comment stating the source and how it was corrected. The final totals at the bottom which included the corrections had a \$0.00 variance. **No issues noted.**

**Key Control 3 - (Occurrence)** - We reviewed the year end adjustment for unearned revenue due to pre-registration of summer and fall quarters. Lee Grubb provided us with the "2024 Unearned Revenue Entry 2024-07-17" spreadsheet detailing the calculations and support for the year end adjustment. The spreadsheet had each college broken down with totals moving (Debit Revenue, Credit 2040010) to record the revenue as unearned as of June 30th. The "Upload 7.1.2024" tab detailed the total for all three which balanced to \$0.00 as the credits equaled the debits. The total amount moved was \$19,554,089.95, which we confirmed by reviewing JV0000487933 in ctclink, which was processed for that amount on 07/01/2024 with the description of "2024 Unearned Revenue Entry". **No issues noted.**

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **J.2.PR.G - Community & Tech College Testing - Seattle**

*Procedure Step:* IT Control Testing - Charges for Services

*Prepared By:* MRF, 10/17/2024

*Reviewed By:* RKM, 10/28/2024

# State of Washington

## Purpose/Conclusion:

### **Purpose:**

To determine whether automated tuition calculation (**key control 1 for ctclink**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls. We also noted the following issue: [V: Seattle Colleges Lack of Documentation for General IT Control].

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [Charges for Services - Controls].

## Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

# State of Washington

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

## State of Washington

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3

# State of Washington

is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

## Software Calculation:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## STEP 6: Final Control Risk

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## Recommendation Review Requirement

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## PUBLIC REQUEST EXEMPTION

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the**

# State of Washington

**Public Records Act. As such, distribution of this record is limited ".**

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **STEP 1: Understand Automated Key Control**

**Significant System:** Charges for Services- Tuition Revenue

**Key Automated Control:** The College's ctcLink subledger, Campus Solutions, creates student's class schedules which then automatically

# State of Washington

calculates tuition and fees, based on student data, tuition codes, and tuition rates set up within the system to ensure tuition and fees due are properly calculated.

Our understanding of the overall control is documented as part of our understanding of controls over relevant assertions for ctcLink in the "Charges for Services - Controls" step.

## Term Rollover and Tuition Updates

The calculation of student tuition and fees is automated in the ctcLink system based on rate tables. There are two types of rate tables that need to be updated and manually reviewed; SBCTC tuition rates and college specific fees. SBCTC updates the statewide tuition and required fees for students. SBCTC updates these rates each year in a programmed upload and performs their own verification of the data adjustments. SBCTC will provide the verification spreadsheets to the Colleges based on academic year and the college retains a copy for their own verification purposes. The College specific fees may get updated on an annual and term basis, so the implementation and review process is called "term rollover". At the end of each fiscal year, the departments work to create their operating budget, which includes a discussion if fees or charges need to change (increase or decrease) or if there are any new charges. These fees include the College wide charges, such as the technology fee charged to every student, as well as course specific fees, such as charges for art classes or science lab materials. The departments submit their budget and fee adjustments to the board each year, where the board votes to approve or deny by July 1st.

## **STEP 2: Confirm and Test Automated Key Control:**

We confirmed and tested the key automated control as follows, to determine whether the automated controls can be relied upon:

To confirm the automated control we recalculated the ctcLink calculated student tuition & fees amounts on a sample of student accounts at: [Charges for Services - Testing]. *No issues noted.*

## **STEP 3: Understand General IT Controls**

The tuition revenue calculation processing resides within a third-party vendor application system, which cannot be modified by system users. The only way for college users to affect the calculation is through edits to associated data tables and screens, and many of those tables are restricted to modification by State Board at the college level.

After it is determined fees need to be adjusted, the departments work with Mark Baumann, Campus Solutions Data Manager, to get the correct amounts into the ctcLink system. Mark is responsible for ensuring that each term, any/all changes have been correctly implemented. He and his team perform judgmental recalculations using ctcLink queries for a variety of scenarios to ensure all the fees and charges are working together correctly, and are being pulled accurately from the updated tables, from both the College specific charges and the statewide SBCTC tuition charges (**Key General IT Control**).

## **STEP 4: Confirm Key General IT Controls**

**Key General IT Control:** Mark Baumann, Campus Solutions Data Manager, and his team perform judgmental recalculations using ctcLink

## State of Washington

queries for a variety of scenarios to ensure all the fees and charges are working together correctly, and are being pulled accurately from the updated tables, from both the College specific charges and the statewide SBCTC tuition charges. We received a walk through of their process on 09/16/2024 via Teams.

At this time, the process is informally recorded as chats in Teams and documentation of review and approval was unavailable for review. We will recommend the College retain specific documentation of this review process. See issue here [[V: Seattle Colleges\\_Lack of Documentation for General IT Control](#)].

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at **MAX**.

### **J.2.PRQ - Community & Tech College Testing - Seattle**

*Procedure Step:* Charges for Services - Testing

*Prepared By:* MRF, 10/16/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion:

#### **Purpose:**

To determine whether reported revenues represent actual amounts relating to the period (Occurrence).

To determine whether revenues were reported at properly valued or calculated amounts (Valuation).

#### **Conclusion:**

We determined the revenues were calculated correctly, and reported correctly in the applicable period. *No issues noted.*

Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.



# State of Washington

For revenues received from the State Treasurer, trace reported amounts to the State Treasurer confirmations available in LGCS.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

## **Cut-Off / Revenue Recognition**

Test a sample of underlying transactions to verify the revenue was recorded for the proper period. Note: transactions at the beginning and end of the period would generally be considered at highest risk of being improperly recorded in the current period.

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

## **Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

## **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Calculation**

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

## **Realizable Value**

## State of Washington

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### **Estimation / Recognition**

Review calculation and support for assumptions of any estimated revenues.

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

Guidance/Criteria:

Record of Work Done:

### **Significant Balances and Assertions:**

Governmental Activities - Education - Higher Education Charges for Services - Occurrence, Valuation

Higher Education Special Revenue - Charges for Services - Occurrence, Valuation

Controls are documented in the "Charges for Services - Controls" step.

### **Selection Methodology:**

Lee Grubb, Assistant Director of Financial Services, provided a "FY24 SF to GL Tuition Revenue Tie-out 2024-09-30" spreadsheet. The pivot table on the first tab listed every account and summarized amount and tied to the reported total by ctclink. Lee also provided a listing of all registered students by ID number and their associated tuition, fee and misc charges in each quarter in the period. Because not all registered students enrolled in classes or paid fees, we filtered the listing to include only students who were charged tuition in at least one quarter and excluded non-academic fees charged to students. See "Pop Completeness" tab, orange highlighted section here [[Confidential Charges for Services](#)]. We used a random number generator to select active students from this population in accordance with the sampling spreadsheet.

### **Substantive tests performed to meet the Occurrence assertion:**

See testing here [[Confidential Charges for Services](#)] on the "Charges for Services" tab.

## State of Washington

We reviewed the account statement for each student and noted the quarter and date paid for tuition and fee charges were recorded in the correct period. ***No issues noted.***

### **Substantive tests performed to meet the Valuation assertion:**

See testing here [[Confidential Charges for Services](#)] on the "Charges for Services" tab.

For each of the selected students/quarters, Lee Grubb (Associate Director of Student Financials) provided us an excel document with pivot table breaking down the fees. She also provided screenshots of the students Bio/Demo data with their ID number, resident status, and path of study (undergrad etc). The enrollment summary for each student listed what classes they took (or dropped) and the number of credits. Screenshots of course-specific sub fees showed if enrolled classes had any additional charges.

International students are charged tuition and fees in ctclink, but all international contract fees are *recorded* as International Contract Revenue (account 4021065). In the support workbook, we were provided with the fee coding for international students through the period and were able to filter the data to see the charges. We confirmed international students were charged the correct amounts, paid the charges, then the amounts were converted to Contracted International revenue. This results in only the fees being reported as standard tuition in the population and on the testing spreadsheet. We traced tuition charges for international students with no issues noted.

We recalculated the charges made to each student using the WA State CC Tuition and Fee rate tables and the provided information (Valuation). ***No issues noted.***

### **J.2.PRG - Community & Tech College Testing - Seattle**

***Procedure Step:*** Education Expenses - Controls

***Prepared By:*** EZM, 10/28/2024

***Reviewed By:*** RKM, 10/28/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

#### **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls.

# State of Washington

Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

## **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

## State of Washington

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

### **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

## State of Washington

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

# State of Washington

## **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities- Education - Higher Education Expenses- Occurrence, Classification

Higher Education Special Revenue - Charges for Expenses- Occurrence, Classification

See lead sheet at: [[Lead Sheet](#)]

## **STEP 1: Gain an Understanding of Internal Controls**

### **Payroll:**

On September 10, 2024, we met with Petrina Sims, Payroll Manager, to gain an understanding of internal controls over payroll expenses at the College. The College utilizes the Human Capital Management Pillar in the ctcLink system to process bimonthly payroll transactions. The system has automated approval levels for employee timecards and changes to payroll such as modifications to existing salary or positions. The college also utilizes an internal district wide shared spreadsheet titled "District Wide New Hire Additional Assignment Spreadsheet" to also track any updates and capture all payroll changes, new positions requested, combo code or budget account coding updates, notes, and payroll related requests. It is shared by management in human resources, payroll and benefits, departments, and the business office. Contracts for regular salaried employees, and faculty are entered into the system by Petrina Sims, Payroll Manager, and approved by college department managers and the employee.

Stipend amounts are processed differently depending on whether the individual is part-time faculty or not. If the individual is a part-time faculty member, the stipend is processed through the Faculty Workbook system in ctcLink and approved by the dean of the department or the department manager. If the individual is a student, exempt staff, or full-time faculty, their stipend is processed through OnBase, which the College switched to in February of 2024. With this system, the stipend amounts are approved by the same individuals, and then sent to the business office to check the combo code budget, and then once the business office approves it, it's sent over to payroll and entered into the system **(Key Control #1 - Occurrence, Classification)**.

New hourly, student, and part time positions such as faculty must be submitted by the program manager or hiring manager for the department using a new hire request form specific to each campus location, and any changes in the system must be supported by approved documentation, such as salary placement forms and documented approval by the supervisor or dean.

Time sheets are filled out in the ctcLink system by employees each pay period. Use of paid time off must be requested through employee self-service and approved by the employee's supervisor in management self-service. Once the employee submits the time sheet, it is automatically routed to the supervisor for approval. Once the supervisor electronically approves the time sheet it is routed to payroll **(Key Control #2 - Occurrence)**.

SBCTC has provided the colleges with a 67-step checklist for processing payroll. Petrina Sims confirmed that the checklist is utilized each pay

# State of Washington

period to ensure complete processing and resolve errors.

## **Initial Setup (steps 1-2)**

## **Process Absence and Time & Labor (steps 3-14)**

## **Process Payroll (steps 15-53)**

## **Confirm Payroll (steps 54-57)**

## **Post-Confirm Tasks (steps 58-67)**

Petrina Sims and Michelle Large, Benefits Specialist, prepare reconciliations each pay period for gross earnings, total deductions, and earnings by pay type using system reports. Annie Butler, Director of Compensation and Benefits, reviews these reconciliations to ensure there are no errors. Accounting also performs a review of these reconciliations and will send them back to payroll if they discover any errors. The college is not currently able to restrict overtime due to staffing levels, but the system will automatically calculate over time rates based on the employee's timecard, which is approved by the employee's supervisor.

## **Accounts Payable:**

On September 11, 2024, we met with Ulrike Lopez, Accounts Payable (A/P) Supervisor, Charlene Rios, Director of Accounting, and David Williams, Director of Financial Reporting, to gain an understanding of the disbursement processes and internal controls over accounts payable at Seattle Colleges.

The A/P department processes various types of disbursements such as vendor payments, student refunds, payroll vendor payments, and travel reimbursements in the form of checks, ACHs, and wires. Vouchers are entered into the accounts payable module of ctcLink based off original invoices or A19s for capital projects or state agency payments.

Original invoices and A19s are scanned and uploaded into the system by A/P staff and attached to each voucher (**Key Control #3 - Occurrence**). Any item ordered from vendors that is over \$3,500 must go through the purchase requisition and purchase order process. All vouchers and purchase orders must go through the ctcLink Approval WorkFlow Engine (AWE) for review and approval and budget check before they can be paid (**Key Control #4 - Classification**).

If receiving is set to be required in the system for items on a PO then an A/P staff member will enter the receipt documentation into ctcLink once the item has been received. If a PO is not in place, such as for items under \$3,500, then the invoice is not entered until the department sends it to A/P. Departments do not send invoices to A/P unless the item has been received.

The college has an internal form titled "Seattle Colleges ACH Request Form" they send to vendors requesting ACH payments instead of checks. The vendor fills it out and returns it to the college. This information is entered into ctcLink by Ulrike Lopez. Ulrike verifies that the vendor's information is accurate by calling the vendor's Accounts Receivable department and cross checking the information on the invoice.



## State of Washington

Duplicate payments are prevented by ctcLink based on invoice numbers - if a duplicate invoice is entered into the voucher entry system, the system will flag it and not let staff go past that point, alerting the user that the invoice number has already been entered into the system. However, the invoice number can be overridden. Ulrike stated that happens when they need to enter a credit for an invoice already in the system - they put the letters "CR" next to the original invoice number to document that the transaction is a credit to the original invoice.

Checks and ACH's that are approved and ready for payment go through a pay cycle that will only pick up payments in approved and/or matched with PO and receipt if required status. Ulrike Lopez then reviews a check register report to verify the list of checks and ACHs to be processed that day - she goes through the report and looks at each check that was printed to make sure they were all accurately printed and that all addresses are appropriate and all checks are accounted for. The A/R staff receives this report from A/P and then the checks are printed in the A/R department. Check stock is stored in a locked cabinet.

All payments are reconciled using the daily and monthly reconciliation processes.

The supplier and vendor lists in PeopleSoft are maintained by the SBCTC and each individual college. They all share this list and can enter vendors and location updates. Once a supplier is entered or updated, it is set to unapproved, and it goes through an approval process by a system support staff member at SBCTC. W-9s are required to be attached, and TINs must match the W-9 from the vendor.

### Key Controls:

**Key Control #1 (Occurrence, Classification)** - Modifications to employment, which affect payroll combo code budgets, are supported in ctcLink and an E-form as necessary and all changes are required to be approved in the system. These modifications include the effective date and payment dates and combo code strings, which ensure that expenses are properly recognized in the correct period and fund.

**Key Control #2 (Occurrence)** - Timecards are created by employees and approved by their supervisors, verifying time worked during the pay period.

**Key Control #3 (Occurrence)** - Original invoices or A-19s are attached to the voucher so the approver can view before approving.

**Key Control #4 (Classification)** - If a voucher is created from a Purchase Order, the approver can review the budget account coding prior to approval. If the voucher is not created from a PO, then the budget account coding is determined by the department submitting the invoice to A/P. All vouchers and POs are required to pass budget check before payment can be made.

### Identified Weaknesses:

None.

## **STEP 2: Confirm Key Controls**

**Key Control #1 (Occurrence, Classification)**- Modifications to employment, which affect payroll combo code budgets, are supported in ctcLink and an E-form as necessary and all changes are required to be approved in the system. These modifications

## State of Washington

**include the effective date and payment dates and combo code strings, which ensure that expenses are properly recognized in the correct period and fund.**

We reviewed the contract audit history for employee ID#101025345 for contract 0632237161 to teach a Physics course during the Fall Term 2023. The total contract amount was \$12,198.67 paid out in 6 payments. The contract was generated in the Faculty workload module of the CTCLink system on September 25, 2023 by Star Conrad at 2:40 p.m. The contract was approved by Vashti Bryant on September 26, 2023 at 2:00 p.m. and also on October 3, 2023 at 10:08 a.m. by Timothy Lorentz. The employee, Azita Seyed Fadaei, accepted the contract on October 3, 2023 at 10:14 a.m. Per the contract, payments were to be made from 10/10/2023 through 12/22/2023. We inspected the paycheck detail report for this employee, and we confirmed that all of these payments occurred during the period.

We also reviewed an EForm for deliverables for grant 21-CDG-597, for FT Faculty, employee ID#201972250. The stipend was the semi-monthly amount of \$2,200 (total contract amount was also \$2,200). The form noted the budget account coding: Operating unit: 7060, Account: 5000070, Fund: 149, Class: 045, Department: 11125. The percentage was 100% and there was a combocode of 000210756. Approval was noted in the signature log at the bottom as follows:

**Key Control 2 (Occurrence) - Timecards are created by employees and approved by their supervisors in the system, verifying time worked during the pay period.**

*No issues noted.*

We reviewed the time cards for employee ID 202553267 and a pay stub, for 10/1/2023 - 10/15/2023 in the amount of \$2,457.75. We recalculated the employee's gross wages by hours paid to the employee using the rate on the pay stub for each time sheet. We noted during our review of the pay stub that the employee was paid on 10/25/23, and we therefore determined that the expense occurred during the proper period. *No issues noted.*

**Key Control #3 (Occurrence) - Original invoices or A-19s are attached to the voucher so the approver can view before approving.**

We reviewed voucher #00042604 (11/27/23) in the ctclink system and verified that original invoices (11/27/23) were attached and shown to the approver (11/29/22). We noted that the payment on the invoice occurred on 12/2/2023, and therefore determined that it occurred in the proper period. **No issues noted.**

**Key Control #4 (Classification) - If a voucher is created from a Purchase Order, the approver can review the budget account coding prior to approval. If the voucher is not created from a PO, then the budget account coding is determined by the department submitting the invoice to A/P. All vouchers and POs are required to pass budget check before payment can be made.**

We reviewed voucher #00042604 created from approved purchase order #3064 for produce from Charlie's Produce and verified that the budget account coding was imported directly from the purchase order and that the budget was valid. The voucher was approved and the budget status was valid at the time of payment. The expenditure was charged to fund 148 (Dedicated Local) in ctclink, on the "Voucher" page, and we found

## State of Washington

that this expenditure was charged to the same fund in the Voucher Accounting Line ctcLink query that was pulled for us by David Williams, Director of Financial Reporting. Per OFM's website, fund 148 rolls up into the Higher Education fund, which is the proper fund that this expense should be rolled up into. **No issues noted.**

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

#### **J.2.PRГ - Community & Tech College Testing - Seattle**

*Procedure Step:* Education Expenses - Testing

*Prepared By:* EZM, 10/28/2024

*Reviewed By:* SHW, 11/6/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To determine whether reported expenses/expenditures represent real obligations incurred during the period (Occurrence).

To determine whether reported expenses/expenditures allocated to the proper fund and period (Classification).

#### **Conclusion:**

We determined not all reported expenses/expenditures represent real obligation incurred during the period. **See issue here:** [\[E: Seattle](#)

# State of Washington

Colleges Misstatement of Education Expenses (Payroll)]. **See AOM here:** [Aggregation of Misstatements (GAAP)].

We determined that reported expenses/expenditures allocated to the proper fund and period (Classification).

## Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Detail Roll-up**

Compare totals from general ledger to accounts payable, payroll or other subsidiary software modules.

Review the government's reconciliation of general ledger to subsidiary systems.

### **Fictitious expenses**

Search for manual journal entries that debit (increase) expenditures. Consider testing if any risk indicators are noted.

Evaluate liabilities directly related to expenses for existence. See the existence steps for current and non-current liabilities for testing considerations.

*For example, if the entity reports a self-insurance liability, the auditor might evaluate whether the change in the liability (and associated expense) occurred. Similarly, if a new liability was reported, evaluate whether that liability (and associated expense) actually exists.*

If the entity reconciles recorded revenues and expenses to bank activity, then review monthly reconciliations and evaluate or test reconciling items.

If entity uses a warrant clearing account or payroll clearing account, review the entity's year-end reconciliation of recorded vendor payments and/or payroll payments with disbursements from the clearing account(s).

Test a sample of expenses/expenditures to determine whether the transaction was valid.

Perform analytical procedures on payroll expenses/expenditures. The analysis should include development of an expectation of what payroll should be in the current year due to changes in employees, COLAs, benefits, etc.

Test payroll to see if transactions are properly charged

### **Invalid, Unallowable or Fraudulent Expenses**

*See the testing strategy considerations in the Rights & Obligations step.*

### **Improper Expense Recognition**

Test selected or sampled expenditures recorded in the current period to verify the expense was recorded for the proper period.

# State of Washington

*Transactions at the beginning and end of the period would generally be considered at highest risk of being improperly recorded in the current period. Auditors should consider scanning transactions recorded during these timeframes to identify high risk transactions.*

## **Incorrectly recording expenses that do not meet GAAP criteria**

Review the entity's schedule cross-walking the financial statements to the general ledger and check that any transactions among consolidated funds are eliminated.

Check that transactions among governmental funds and transactions among proprietary funds are eliminated on the government-wide statements.

## **Interfund Expenses**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

The following is a list of **considerations** for testing the classification assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Sample transactions for correct classification. *Use the "Sampling for FS Substantive Testing" spreadsheet available in the Store to calculate sample size and make any projection of likely misstatement to the population.*

If planning has identified a limited population that is high risk (ex: certain transaction types and/or line items within an opinion unit), scan these populations and test selected transactions.

## **Journal Vouchers**

Search for manual journal entries that reclassify expenses/expenditures from one opinion unit to another without recording a balance sheet transaction, other than a direct charge to fund balance (debit and credit to expenditure and fund balance for each opinion unit, respectively). Test selected journal entries based on risk.

Search for manual journal entries that reclassify expenses/expenditures from one line item to another. Test selected journal entries based on risk.

## **Vendor Payments**

Review the top vendors paid by opinion unit or line item (preferably as a multi-year trend) and evaluate whether the vendor meets expectations in relation to the activities of the fund. Test transactions for each unexpected vendor based on risk.

Test selected or sampled transactions for correct classification.

*NOTE: this test may be combined with expenditure tests for other attributes. For example, expenditure testing for accountability or single audit purposes may also be used for classification testing.*

# State of Washington

## Payroll

Scan totals charged to each opinion unit by employee (preferably as a multi-year trend) and evaluate whether the allocation of employee's time to that opinion unit meets expectations based on job titles, organization charts, observation or the phone list. Follow up on unexpected allocations by review of timesheets or employee interviews.

Perform an expected payroll test by opinion unit.

Test a sample of pay periods for salaried and hourly employees to ensure that expenditures are being classified to the correct opinion unit. This test should verify both the correct allocation of direct charges and that leave and benefit costs are allocated in the same proportion as direct charges.

## Cost Allocation Plans / Internal Service Fund Allocations

Review cost allocation plans or internal service fund charges to confirm that the classification of joint costs to different opinion units is supported. *See example testing strategies for these areas located in the Accountability cabinet .*

Guidance/Criteria:

Record of Work Done:

## **Material Balances and Assertions:**

Governmental Activities- Education - Higher Education Expenses- Occurrence, Classification  
Higher Education Special Revenue - Charges for Expenses- Occurrence, Classification

Controls are documented in the Education Expenses\_Controls step.

## **Substantive tests performed to meet the Occurrence and Classification assertion:**

### **Payroll:**

See testing here:[CONFIDENTIAL - Education Expenses]

We tested payroll disbursement transactions to determine whether reported expenses/expenditures represent real obligations incurred during the period and if reported expenses/expenditures were allocated to the proper fund (Occurrence and Classification). During testing we determined if expenses were supported by valid documentation, earn type amounts agreed to the supporting documentation, and that expenses were recorded to the proper fund.

We randomly selected 30 employees from the ctcLink Query CTC\_PY\_PAY\_CHECK\_DETAIL that we obtained from Petrina Sims, Payroll Manager. There were 3,036 employees listed representing a total of \$135,086,442 in gross wages on the report for fiscal year 2024, so we utilized the

## State of Washington

random number generator to select our sampling population.

We requested documentation from the Pertrina such as Faculty Workload Appointment forms, Earnings Account Mapping ctclink screenshots, Stipend Request forms, QHC\_TL\_PAYABLE\_TIME\_STATUS ctclink queries, Employee Compensation History ctclink screenshots, timesheets, and QHC\_AB\_ALL\_LEAVE\_TAKEN ctclink queries to support the gross wages paid to the 30 selected employees at Seattle Colleges. We traced amounts in the supporting documentation to amounts by earn-type for each employee to verify occurrence. We also compared the combocodes found in the Earnings Account Mapping to confirm that wages were properly classified to the correct fund. We also verified gross wages for each employee by earn type using the ctclink query QHC\_PY\_EMPL\_WAGES (one was provided for each employee tested), provided by David Williams, Director of Financial Reporting. We did not receive full support for 7 of our 30 testing selections, resulting in a known misstatement of \$(69,121), and a total misstatement (known + likely) of \$6,869,128. **See issue and AOM linked above in conclusion.**

### **Accounts Payable:**

See testing here:[[CONFIDENTIAL - Education Expenses](#)]

We tested accounts payable disbursement transactions to determine whether reported expenses/expenditures represent real obligations incurred during the period and if reported expenses/expenditures were allocated to the proper fund (Occurrence and Classification). During testing we determined if expenses were supported by valid documentation, amounts agreed to the supporting documentation and that expenses were recorded to the proper fund.

We obtained a query from Ulrike Lopez, Accounts Payable Supervisor: QFS\_AP\_VCHR\_ACCTG\_LINE. The query was a detailed listing of transactions for Objects E - J. We randomly selected 30 transactions to test.

Since we had access to the ctclink system, we were able to utilize the accounts payable module to search for each voucher identification number on our transaction sample list. In the system, we were able to review and verify the approval history for the vouchers, view attached original invoices and A-19s, and review the budget account coding or chart string for each voucher line to ensure it correlated with the associated approved purchase order or the attached A-19. If applicable, we were also able to see receiving information. We were able to verify that the attachment was shown to the approver(s) to indicate that the cost was approved to pay before they approved the payment.

Our selection included some vouchers for US Bank National Association, that did not have approvals and documentation attached. We inquired with David Williams and he let us know that this was actually a Purchasing Card transaction. These transactions also go through the Accounts payable module, however they do not have the documentation attached or the approvals viewable within the accounts payable module. David provided us with additional documentation for these purchase card transactions, and we were able to see that the transactions were properly approved and supported by documentation, and they were properly classified to the correct fund. **No issues noted.**

### **J.2.PRG - Community & Tech College Testing - Seattle**

# State of Washington

*Procedure Step:* Federal Grants in-Aid - Controls  
*Prepared By:* MRF, 9/12/2024  
*Reviewed By:* RKM, 10/18/2024

## Purpose/Conclusion:

### **Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

### **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

## Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

### **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant*



## State of Washington

*deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

### **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.*

### **STEP 4: Control Testing**

## State of Washington

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Education - Higher Education Operating Grants and Contributions - Occurrence  
Higher Education Special Revenue - Federal Grants-In-Aid - Occurrence

See lead sheet here: [[Lead Sheet](#)]

For fiscal year 2024 we noted Department of Education grants and contracts revenue made up approximately 93 percent of the total Federal grants-in-aid balance. Our control understanding and testing will focus on these revenues. We met with David Williams (Director of Financial Reporting), Charlene Rios (Director of Accounting), and Lee Grub (Associate Director of Student Services) on 09/11/2024 to gain an understanding of controls and procedures related to federal grants in aid. We noted that Lee was recently promoted to her position and had previously been the grant manager.

## **STEP 1: Gain an Understanding of Internal Controls**

There are two main types of grant expenditures related to Department of Education (DoE); Financial Aid for students through Pell grants and direct loans and Grants and Contracts for other educational expenses like classroom equipment. Lee estimates that Financial Aid is the far larger expense and revenue.

**Financial Aid:** Financial aid is awarded to students each quarter in packages based on FAFSA (Free Application for Federal Student Aid), the amounts flow through the Student Financials (SF) module in ctclink, and gets posted to student accounts. On a monthly basis, Lee (or her

## State of Washington

replacement Trinity) will pull the GL data and reconcile between the SF module and the ledger.

**Grants and Contracts:** Each grant or contract has a Primary Investigator (PI) who is the point of contact for the grant, conducts funding requests, and authorizes expenditures. When expenditures are entered into the accounts payable module in ctclink, the system requires information about if the expense is related to a grant. If it is, ctclink automatically books the revenue to match the expenditure. Expenditures could be for any related part of the grant such as equipment, scholarships, or staff payroll.

### **Making the Drawdown:**

Each fiscal month end, Lee runs the "QFS\_GL\_JRNL\_ACCT\_ANALYSIS", Program/Organization Trial Balance report for each campus and org index within CTCLink. Each Org index corresponds to a different grant type, with the program/org title describing the specific award. The reports are related to a program/organization trial balance for that month and provide expenditure and revenue amounts. The Grants team creates an invoice to match the expenditures and sends the package of support to the PI (or SF) for approval.

For each grant, revenues and expenses are also tracked in Excel spreadsheets that tracks the YTD expenditures and revenues requested. The generated invoice is approved when the amount reconciles to the calculated monthly drawn-down amount (**Key Control 1 - Occurrence**). When the invoice is approved, the request is sent to the district. For Department of Education funds, the G5/6 portal is used to request funds, for other sources the grant is requested from the source itself. For example, grants from State Agencies are requested through the agency itself. As a district, the college confirms that ACH payments are received as a deposit. In ctclink, approval is required before any funds can be drawn-down.

Lee verifies that the draw-down is received in full by reviewing the daily ACH report from Bank of America. After verifying the receipt, she creates a journal entry to record the revenue in ctclink. She provides the documentation above, including a screenshot of the draw request and ACH statement to Davina Fogg, Executive Director of Finance/Controller, for approval of the batch transactions to record the revenue (**Key Control 2 - Occurrence**).

### **Key Controls:**

**Key Control #1: The grant invoice is generated by the grant team based on true expenditures related to an authorized grant and is approved for available funding each month.**

**Key Control #2: The batch for revenue processing is approved after a secondary review by the Controller, with the screenshot of the draw request, the excel worksheet, and ACH statement showing the expense occurred and was authorized.**

### **Identified Weaknesses:**

None

## **STEP 2: Confirm Key Controls**

**Key Control #1: The grant invoice is generated by the grant team based on true expenditures related to an authorized grant and is approved for available funding each month.**

## State of Washington

We reviewed the grant revenue invoice for Pell financial aid issued in FY 24. Lee Grubb provided the "WA062 Pell Recon" spreadsheet. The "data" tab listed all expenditures through the year, we noted there were 113 rows of data totalling \$5,493,704.09 in expenditures. The "total analysis" tab contained a pivot table of the data with some adjustments, for a total of \$5,493,088.09. It also contained a screenshot from the Department of Education grant website G5/6 showing that the completed payments of Pell grants was \$4,396,256.99. The difference between the total amount expended and total revenue returned (completed payments) was \$765,023.25. However, the tab also showed a screenshot detailing that the only available funding as of that date (because there are frequent timing differences) was \$193,146.01. Since the amount expended is greater than the available funds for drawdown revenue, the total amount of available funds was requested. We reviewed the PDF document "WA062 FY2324 Pell Drawdown Backup" which detailed the request for the full available amount, the generated invoice numbered DRA-0000000705 and confirmation of deposit to the college's BOA account on May 30, 2024. *No issues noted.*

**Key Control #2: The batch for revenue processing is approved after a secondary review by the Controller, with the screenshot of the draw request, the excel worksheet, and ACH statement showing the expense occurred and was authorized.**

We reviewed a screenshot of the approval for the draw down credit Invoice in the billing system. The invoice number matched the workbook of support of DRA-0000000705. We noted it was approved by the central billing approver, Julie Larmore, on 05/30/2024, and by Charlene Rios, approver for expenditures in business unit WA060 if over \$50K on 05/30/2024 two hours later. *No issues noted.*

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **J.2.PR.G - Community & Tech College Testing - Seattle**

*Procedure Step:* Federal Grants in-Aid - Testing

# State of Washington

*Prepared By:* MRF, 10/4/2024

*Reviewed By:* RKM, 10/18/2024

Purpose/Conclusion:

**Purpose:**

To determine whether reported revenues represent actual amounts relating to the period (Occurrence).

**Conclusion:**

We determined reported revenues represent actual amounts relating to the period (Occurrence).

Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

For revenues received from the State Treasurer, trace reported amounts to the State Treasurer confirmations available in LGCS.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

**Cut-Off / Revenue Recognition**

Test a sample of underlying transactions to verify the revenue was recorded for the proper period. Note: transactions at the beginning and end of the period would generally be considered at highest risk of being improperly recorded in the current period.

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

**Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

**Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

## State of Washington

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

Guidance/Criteria:

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

### **BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

Record of Work Done:

### **Significant Balances and Assertions:**

Governmental Activities - Education - Higher Education Operating Grants and Contributions - Occurrence  
Higher Education Special Revenue - Federal Grants-In-Aid - Occurrence

Controls are documented in the "Federal Grants-In-Aid - Controls" step.

### **Substantive tests performed to meet the Occurrence assertion:**

We reviewed AFRS data to determine what revenue sources were significant for testing. We determined source 384 made up 84% of the Federal Grant-In-Aid balance and decided to focus our testing on source 384 (Department of Education). Lee Grubb, Associate Director of Student Financial Services, provided the testing population in the spreadsheet "FY24 Federal Grant Revenue QFS\_GL\_ACCOUNT\_ANALYSIS". We tied the EIS reported amounts for Federal Grants in Aid to the totals of the population query with no variance. See our summary at: [\[Federal Grants In Aid\]](#) tab, "Population Completeness".

We used the FS Substantive Sample spreadsheet with tolerable misstatement and assurance levels dictated by the material balance workpaper for a planned sample size of 30. We selected 1 individually significant item and randomly selected 30 samples throughout FY24. Lee Grubb provided support for each of the grant revenue amounts. Because the selected amounts were per project for a single day, we used the population spreadsheet to filter and find the total amount of the project for the month (period).

We tied the total of the period to the College's monthly grant reconciliation (tied the expenditures to the revenue recorded). Any variances of

## State of Washington

things like overstated expenses were investigated and reversed as appropriate to ensure all revenue tied to expenses. We reviewed email chains between staff members that outlined the identified variances and followed the included screenshots of adjustments and resubmitted workbooks to confirm the adjustment occurred. If multiple projects have the same funding source then the draw amounts were requested in a batch. Lee also provided the draw requests for the totals and bank statements to show the subsequent deposits.

By tying the daily revenue recorded to the monthly batch and confirming dates, we determined reported revenues represent actual amounts relating to the period (Occurrence). See testing at [\[Federal Grants In Aid\]](#), tab, "Grant Revenue Testing". ***No issues noted.***

### J.3.PR.G - Community & Tech College Testing - Spokane

*Procedure Step:* Summary & Conclusion

*Prepared By:* JAG, 10/18/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion:

#### **Purpose:**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

#### **Conclusion:**

We determined that **no modifications** were necessary to inherent risk, control risk or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.



## State of Washington

*If the results of substantive testing indicate a need to change control risk, auditors should also update the [Permanent File](#) by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the [Material Balances](#) spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the [Changes to FS Audit Plan](#) step.*

**2. Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material misstatement. In making this determination, auditors should evaluate:**

Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

## State of Washington

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the "what could go wrong", in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

**[Investments](#) area guide**

Record of Work Done:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

We noted no results from our substantive tests which would indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

We determined that the quality and quantity of evidence obtained was both sufficient and appropriate.

### **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* Cash and Pooled Investments - Controls

*Prepared By:* JAG, 10/7/2024

# State of Washington

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

**Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls. We noted one issue related to a lack of evidenced review and approval of the investment reconciliations. See issue here: [\[V: CCS Lack of Documented Review and Approval of Investment Reconciliations\]](#)

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

**STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

# State of Washington

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

**Expected key control for existence and completeness:** Bank reconciliations are performed timely on at least a monthly basis to ensure the general ledger agrees to bank and investment account records.

*Documentation should include who performs bank reconciliations, how often they are performed and how reconciliations are aggregated and compared to the general ledger.*

*Note: we would expect additional key controls if the government has any alternative investments or investments subject to significant interest rate or other risks.*

Expected compensating controls:

- An accounting system module or a standard template is used to document reconciliations.

- Segregation of duties in that the person performing bank reconciliations does not have cash handling duties or access to initiate disbursements by wire or check.

- Timely, independent review of bank reconciliation documentation, including journal entries for adjustments identified from the bank statements (such as fees, NSF checks, etc).

- An up-to-date listing of change fund, petty cash and imprest fund accounts is maintained in accordance with BARS 3.8.8.

- Zero-balance bank accounts and clearing funds (see BARS 3.8.6) are reconciled to zero on a monthly basis.

- If the government has an investment account (that is, other than the State or County LGIP), documented inquiry with their investment service to verify the methodology for determining fair value of investments and the valuation input hierarchy level for purposes of their fair value (GASB 72) disclosures.

*Some investment accounts provide information about its methodology, assumptions, and data in valuing investments at the asset class level. However, brokers often provide no, or only limited, information about the inputs and assumptions used in developing the fair value. Management should either obtain a document with this information or contact the broker/institution to gain an understanding of the information about methods and inputs used in determining the fair value and where the investment should be disclosed in the hierarchy.*

*Contact the Investment Specialist for any questions on expected controls or documentation over fair value disclosures.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

# State of Washington

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*Suggested confirmation for expected key controls are to obtain and scan all year-end bank reconciliations and supporting documentation. This is normally done in conjunction with substantive testing. We would expect that bank reconciliations would clearly show check figures that compare the aggregated adjusted bank balance to the general ledger.*

## **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

## **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the*

## State of Washington

*audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

**Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Higher Education Special Revenue Fund - Cash and Cash Equivalents - Existence

Higher Education Student Services Fund - Cash and Cash Equivalents - Existence

See lead sheet here: [[Lead Sheet](#)]

**1. Gain an Understanding of Internal Controls**

On 9/12/2024 we met with the following people to discuss internal controls over cash and investments:

Tiffany Henderson, Director of Financial Reporting

Laurice May, Fiscal Analyst 2

Clint McGregor, Fiscal Services Account Manager

**Cash**

CCS has had no changes in FY24 to their list of cash bank accounts, which are:

Bank of America Checking

Bank of America Sweep

Washington Federal Bank (Checking)

Mount West/Glacier (Savings)

USBank Business Silver (Money Market)

The BoA accounts are CCS' main accounts with the most daily activity. Daily, Laurice (FA2) will download account information (daily deposits, ACH, checks, adjustments, EFTs, etc.) from the BoA's website using the CashPro tool in order to reconcile the day's transactions. She imports the file from BoA into ctcLink. SBCTC also goes to the BoA website and imports the transaction file into ctcLink so Laurice can compare her version, to SBCTC's version, then to the GL in ctcLink. As the data in ctcLink does not give a lot of specific detail about each transaction, Laurice uses the information from BoA to create detailed entries called "Treasury journal entries" to post to the GL. To ensure proper segregation of duties, staff who receipt cash have no access/input to the bank reconciliation process.

## State of Washington

At month end, Laurice performs the reconciliation for all cash counts except for Bank of America Checking. A separate reconciliation is prepared for the Bank of America checking account and this reconciliation is prepared by Clint McGregor, Fiscal Services Account Manager, and reviewed and approved by Tiffany Henderson. Typically, there are multiple bank activities that need to be reconciled. CCS has found that reconciling the journals by type has helped them to complete more accurate bank reconciliations. After Laurice prepares the reconciliation then Clint reviews and approves it to ensure it is accurate **(Key Control 1)**. At year end, a similar process is performed as with month end, but Tiffany also performs a review of the entire year's reconciliations.

For petty cash, approximately once a month Clint prepares a tracking spreadsheet based on petty cash counts from each of the cash receipting locations. This information is compiled by Tiffany. Clint will compare this data to what is in the GL in ctcLink to ensure amounts are recorded correctly in the system.

### Investments:

CCS has the following investment accounts:

LGIP

Banner Bank (Tiffany noted during the control meeting that the two CD accounts with Banner Bank matured in February so they were moved to a money market account.)

USBank Safekeeping (Money Market)

Once a month Clint prepares a monthly reconciliation of investment accounts. He receives investment account statements from Tiffany and LGIP statements from the CFO. Once his reconciliation is complete, showing CCS' monthly position, he sends the reconciliation to Tiffany for review and approval **(Key Control 2)**. Once approved, Clint prepares the journal entries to post to the GL. These entries are reviewed and approved by the CFO prior to posting.

At year end, Clint takes the investment statements from the entire year and compares the actual statements to the GL to make sure that all activity has been accounted for in the GL. Once the year end reconciliation is prepared, Tiffany reviews and approves it to ensure it is accurate.

### Historical Information:

During 2019, the State Board force closed each FY from 2016 through 2019. In order to bring the balances back to current for the start of 2020, the College performed several entries to write off cash balances which were growing due to the issues in ctcLink. In FY19 we were shown a CASH spreadsheet which showed the adjustments made in 2019 that were applicable for 2016, 2017, 2018 and 2019. In order to do this, the College created a summary of amounts to be adjusted, and then took amounts out of the cash accounts (101150, 101151, 101160), into 342700 and then out of 342700 and into 603372 for prior period adjustments. The total amount of adjustments made were:

2016 - \$5,318,010.03

2017 - \$6,143,096.53



## State of Washington

2018 - \$9,001,754.39

2019 - \$14,277,483.62

Total adjustments made in 2019 = \$34,740,344.57

There were no write offs for 2020, 2021, 2022, 2023, or 2024. For controls to ensure that the GL is reconciled to AFRS see: [[Controls - ctcLink System Reconciliation](#)]. This is done at the state level.

### Key Controls:

**Key Control #1 (Cash - Existence):** Monthly, the Fiscal Analyst 2 prepares a reconciliation of cash bank accounts between bank statements and the GL to ensure recorded cash amounts represent actual assets. The Fiscal Services Account Manager reviews and approves the reconciliation to ensure its accuracy.

**Key Control #2 (Investments - Existence):** Monthly, the Fiscal Services Account Manager prepares a reconciliation of investment account balances to ensure all account activity from the statements is accounted for in the GL. The Director of Financial Reporting reviews and approves the reconciliation to ensure its accuracy.

### Identified Weaknesses:

**None.**

### **STEP 2: Confirm Key Controls**

**Key Control #1 (Cash - Existence):** Monthly, the fiscal analyst 2 prepares a reconciliation of cash bank accounts between bank statements and the GL to ensure recorded cash amounts represent actual assets. The Fiscal Services Account Manager reviews and approves the reconciliation to ensure its accuracy.

We reviewed the June 2024 reconciliations for all bank accounts. We noted the following:

Washington Federal 1000080: Prepared by Laurice May, Fiscal Analyst 2 on 7/11/2024. Reviewed by Clint McGregor, Fiscal Services Account Manager on 7/11/2024.

Mountain West 1000090: Prepared by Laurice May, Fiscal Analyst 2 on 11/8/2023. Reviewed by Clint McGregor, Fiscal Services Account Manager on 11/10/23. The reconciliation states that this account was closed on 10/17/23 and we reviewed the closure documents to confirm.

Bank of America Sweep 1000100: Prepared by Laurice May, Fiscal Analyst 2 on 7/11/2024. Reviewed by Clint McGregor, Fiscal Services Account Manager on 7/11/2024.

US Business Silver 1000110: Prepared by Laurice May, Fiscal Analyst 2 on 7/11/2024. Reviewed by Clint McGregor, Fiscal Services Account Manager on 7/11/2024.

Bank of America Checking: 1000070: Prepared by Clint McGregor, Fiscal Services Account Manager on 7/22/2024. Reviewed by Tiffany Henderson, Director of Financial Reporting on 8/2/2024.

**No issues noted.**

# State of Washington

**Key Control #2 (Investments - Existence):** Monthly, the Fiscal Services Account Manager prepares a reconciliation of investment account balances to ensure all account activity from the statements is accounted for in the GL. The Director of Financial Reporting reviews and approves the reconciliation to ensure its accuracy.

We reviewed the "FY24\_Investment\_Workbook.xlsx" which included the June 2024 Investment Reconciliation. We noted the reconciliation included activity for all investment accounts. There was evidence of Clint McGregor, Fiscal Services Account Manager, preparing the report on 7/2/2024. The reconciliation did not contain evidence of a review.

**We recommend CCS ensure all reconciliations include a signature and date of review to evidence that the review and approval has taken place and in a timely manner as required by SAAM 85.50.40.c. See issue here: [\[V: CCS Lack of Documented Review and Approval of Investment Reconciliations\]](#).**

## **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* Cash and Pooled Investments - Testing

*Prepared By:* JAG, 10/16/2024

*Reviewed By:* RKM, 12/10/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To determine whether reported cash and pooled investments existed as of the end of the period (Existence).

**Conclusion:**

We determined reported cash and pooled investments existed as of the end of the period.

Testing Strategy:

**SAO Policy Requirement: Confirming or Verifying Cash & Investment Balances**

Confirmations can either be blind or a positive confirmation. In a blind confirmation (sweep), the auditor requests information on all accounts the bank holds for the entity (by entity name and/or EIN). In a positive confirmation, the auditor lists accounts (or accounts and balances) per the entity and asks the bank to confirm that the information is correct.

Confirm cash and investment account balances with County Treasurer, bank and/or brokerage. Use the template confirmation form provided in the Store when needed.

Confirmations can be mailed to addresses listed on the Bank Confirmation Address List available on the Auditor Reference Guide. If the bank notifies you of a different address, please contact Team Audit Support to update the list.

Banks may confirm incorrect amounts either due to a simple mistake, use of a wrong confirmation date or incorrectly including or excluding accounts. The first step in resolving differences should be to check information against the entity's bank statements and then call the bank to specifically confirm any difference.

Confirming investments may involve physical inspection, confirmation with the issuer, confirmation with the custodian, confirmation of unsettled transactions with the broker/dealer, confirmation with the counterparty, and/or reading executed partnership or similar agreements. When confirming investments, ensure investments are held in the entity's name.

*If confirmations are not used*, auditors must at minimum verify balances to the County Treasurer, bank and/or brokerage statements. If this is done, the auditor should consider the risk that the statements were altered and should examine papers for indications of alteration.

The following is a list of **additional considerations** for testing the existence assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

**Bank Reconciliations**

If the auditor is comparing reconciled (confirmed) bank or county treasurer balances to the GL (rather than confirmed amounts within an

## State of Washington

expected variance due to reconciling items), the auditor should consider performing some or all of the following tests to verify the accuracy of the reconciliations. Note that testing the reconciliation will provide evidence of both the existence and completeness of cash and investment balances.

Trace (or compare summed) bank balances per statements to reconciliations.

Trace (or compare summed) book balances per reconciliations to the general ledger or financial statements.

*If a cash account is allocable to a particular fund, the balance in the general ledger should be recorded in the same fund.*

Scan the reconciliation for reasonableness. Look for unusual, unexpected or vaguely described reconciling items, lack of support or detail, very large reconciling items, very old reconciling items, and missing or extra elements that would indicate that the reconciliation was being performed incorrectly.

Foot the reconciliation for accuracy.

Trace deposits in transit to the subsequent month's bank statement, considering reasonableness of the in-transit period.

Trace outstanding checks to cash disbursement journal.

Check that any other reconciling items are valid and have been properly accounted for (ex: large debit or credit memos).

Check reconciliation against prior and/or subsequent reconciliations for reasonableness of amounts and items included and to trace reconciling items from the previous and/or subsequent period.

### Other Tests

Inquire whether any checks or deposits were being held at year end for budget, cash flow or other purposes.

Confirm investments purchased but not received as of year-end

Confirm investments sold but still held as of year-end

Confirm interest due or accrued but not yet received as of year-end

Search for manual journal entries that debit (increase) cash. Consider testing if risk indicators are noted.

Review reconciliations of clearing and transmittal accounts.

See accountability steps for testing strategies related to petty cash and imprest funds, which are not expected to be material to the financial statements.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

Guidance/Criteria:
--------------------

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Outstanding Checks and Deposits in Transit** – Per TIS section 1100.08 (AICPA Technical Questions and Answers), outstanding checks should be reported as a reduction of cash and the amount of deposits in transit should be reported as cash. A check is considered outstanding from the time that it is out of the payor's control – when mailed or delivered to the payee – until the time it clears the bank. Cash should represent amounts within the control of the reporting entity, that is, the amount of cash in banks plus cash and checks on hand and deposits in transit minus the amount of outstanding checks.

**SAO Audit Policy [6350](#) – External Confirmations**

**[Investments](#) Area Guide**

**[LGIP Fund Summary Reports](#)** - includes a list of local government accounts and balances in the Local Government Investment Pool

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.8.6](#) Use of Payroll and Claims Funds**

Record of Work Done.
----------------------

## **Significant Balances and Assertions:**

Higher Education Special Revenue Fund - Cash and Cash Equivalents - Existence  
Higher Education Student Services Fund - Cash and Cash Equivalents - Existence

Controls are documented in the "Cash and Cash Equivalents - Controls" step.

## **Substantive tests performed to meet the Existence assertion:**

See testing here: [[Cash and Investments Testing](#)]

AFRS to ctcLink:

We obtained ctcLink data using the query QFS\_GL\_SNP\_DETAIL, filtered for cash and investments and AFRS data from here: [[Final Planning Community Colleges Selected for Testing](#)]. We determined that the AFRS balances tie to ctcLink without exception. However, due to the complexity

## State of Washington

of testing the AFRS amounts individually we decided to test the College's entire cash and pooled investments balance to determine if it existed as of June 30, 2024. The main focus of testing is GL titled, "Cash - Bank 1" since this GL consisted of most of the AFRS balances we selected. This GL account is the College's main Bank of America checking account. See tab, "AFRS & ctcLink" at: [\[Cash and Investments Testing\]](#).

### Cash & Investments Summary:

We obtained June 30, 2024 month-end reconciliations, bank/investment statements, and petty cash reports from Tiffany Henderson, Director of Financial Reporting, to verify existence of cash and pooled investments as of 6/30/2024. Additionally, we obtained the July and August 2024 bank statements to verify reconciling items and outstanding checks. See summary on tab, "Cash & Investment Summary" at: [\[Cash and Investments Testing\]](#).

### Outstanding Checks:

For outstanding checks, we obtained the Bank of America outstanding check report (ctcLink). We noted the balance of outstanding checks on the outstanding checks report tied to the Bank of America reconciliation prepared by the College. Additionally, we used the Financial Audit Substantive Sample testing spreadsheet to randomly selected 38 outstanding checks and reviewed either the July outstanding check report or July 2024 bank statement to ensure the checks were either still outstanding or were paid in July 2024. See tab, "Outstanding Checks Testing" at: [\[Cash and Investments Testing\]](#). We determined outstanding checks at fiscal year end either cleared the following month or were still documented as outstanding. ***No issues noted.***

### Deposits in Transit:

We traced all of the deposits in transit to the July 2024 bank statement and determined the bank statements and what was documented in the college's bank reconciliation for deposits in transit align. ***No issues noted.***

### Reconciling Items/Adjustments:

We traced the following two adjustments to the July 2024 bank statement and an AR items spreadsheet, and determined what was documented in the college's bank reconciliation aligns:

Pay cycle in transit: \$133,450.79

AR Reconciling Items: (\$326,967)

The College had two other reconciling items that could not be traced to the GL or bank statements. After follow up with Tiffany Henderson, we found that one item was an ongoing issue due to the amount being an off book audited balance adjustment from FY23 related to cash over/short entries from previous fiscal years that were reported incorrectly to the GL. The other item was also an ongoing issue related to the VPA process for state allocation. The College is currently unable to reconcile and complete a draw because SBCTC isn't allowing any draws due to their process change. The College is currently working with SBCTC to resolve these issues. ***The error is below the floor.***

# State of Washington

## J.3.PR.G - Community & Tech College Testing - Spokane

*Procedure Step:* Depreciable Capital Assets - Controls

*Prepared By:* NJH, 9/23/2024

*Reviewed By:* RKM, 10/10/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

**Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

**STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

## State of Washington

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

### **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***



# State of Washington

## **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

## **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with***

# State of Washington

*the AIC or AAM, since they must be reported as findings.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

## **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Depreciable Assets (Net of Accumulated Depreciation) - Existence, Valuation

See lead sheet here: [[Lead Sheet](#)]

## **STEP 1: Gain an Understanding of Internal Controls**

On September 16, 2023, we met with Yabing Fisher, Expense Senior Accountant, and Tiffany Henderson, Director of Financial Reporting, to gain an understanding of internal controls over depreciable capital assets.

CCS follows the SAAM, Chapter 30, for guidelines on what to capitalize and determining appropriate useful lives. We reviewed the SAAM at <https://www.ofm.wa.gov/sites/default/files/public/legacy/policy/30.20.htm> and noted the following:

Threshold for capitalizing assets is \$5,000 for furniture/equipment and library resources.

Buildings, building improvements, improvements other than buildings, and leasehold improvements with a cost of \$100,000 or greater are capitalized, however, land and construction in progress are non-depreciable capital assets.

The Community Colleges of Spokane mainly uses the ctLink Asset Management (AM) Module for asset tracking and automatically calculating straight line depreciation.

## State of Washington

### Additions:

For small and attractive assets, CCS uses an inventory control system called TME, which is software that is used in tandem with AM in ctcLink to track assets. TME does not calculate depreciation, but is rather a way of keeping tabs on small assets that the college owns. Most new assets are added by Debra Griffin, Surplus/Inventory Control Specialist, to the TME and AM module, with information gained from communication between Debra and the purchasing department. When a department decides to purchase a new capital asset, it begins similar to all expenditures/purchases with a Purchase Requisition in ctcLink. Purchasing contacts Debra and requests a profile ID and state tag number for the asset to add to the purchase requisition. The profile ID is what designates the asset's useful life as determined by the SAAM for that asset category. Debra reviews the information on the requisition for accuracy and sends it back to purchasing for them to turn the requisition into a purchase order. Once the purchase order is complete, it is routed back to Debra for review and approval. Debra maintains a list of all pending purchase orders with state tags and as they are received by Central Services or delivered on site, she tags the asset for inventory. Then Debra adds the asset to AM and also to TME if applicable. Information added includes the profile ID, item description, serial number, location, cost (per invoice), date of acquisition and other pertinent information about the item (**Key Control #1 - Manual - Existence / Valuation**). Yabing receives an email that includes a list of all additions and retirements every month. Although there are no secondary checks/reviews when Debra is entering asset information into AM (or TME), Yabing reviews this list to ensure that everything ties to what is in the AM module system. Yabing reviews information from an accounting perspective and she is authorized to go into the systems and make corrections if necessary.

### Disposals:

When a department decides to dispose of equipment, the manager of the department submits a "Property Disposal Request" form to Debra at the Central Services Office. The Central Services department then processes the request by putting the item in their queue for pick-up. Once surplus equipment arrives at the Central Services warehouse, Debra will determine what the disposition will be:

- Online Auction with Department of Enterprise Services for general and some specialized equipment

- Reinland Auctions for vehicles, heavy equipment, specialized industrial trades equipment

- Recycle for salvage

- Disposal for items with no sale or salvage value

Debra is responsible for the tracking of tagged assets. Once the determination is made to remove the asset from service, she gives it a general authority number to track it and retires the asset in ctcLink AM module using the "RET" transaction type. Jeff Stradley, The Logistics Manager, approves all retirements by signing the Property Disposal Request form. All documentation is stored at Central Services. Debra will also send a fixed asset retirement report to Yabing every month. Yabing reconciles disposals on a monthly basis (as mentioned above in additions, she is included on a monthly email that includes the list of that month's additions and retirements). She verifies the asset was appropriately removed from the TME and AM systems and processes a JV in the GL to reflect the activity. Within ctcLink AM module, the movement of the asset to retirement ("RET") creates a system-generated JV, which is processed (reviewed and posted) by Yabing. JVs for additions, retirements, and depreciation are a monthly, system generated process and SBCTC discourages colleges from making manual modifications to these system generated JVs.

# State of Washington

## Capital Facilities - Buildings & CIP:

Building additions/disposals are initiated within CCS' Capital Facilities department who is responsible for creating purchase requisitions and working with the budget department to determine the overall plan of construction for a new building. The building is tracked in the AM module and listed as CIP until finished when it is placed in service. When construction begins and payments are made to vouchers, the capital facilities team will assess payments and approve them for expenditures to be capitalized and added to AM. Expenditures for capital assets are flagged as a capitalizable asset upon purchase and based on construction phase. CIP is capitalized at fiscal year end. Yabing works with the capital projects team to determine which projects have been completed and which are still in progress. Yabing performs a detailed reconciliation by project ID using data from the GL to determine amounts to report as CIP at FYE.

## Depreciation:

The College relies on the depreciation calculated by the ctclink system. The straight line method using no salvage value is used for all asset depreciation calculations. The ctclink system automatically calculates depreciation based on profile types and the asset information entered within the Asset Management module: in-service date and asset value/cost (**Key Control #2 - Automated - Valuation**). An entry is created and posted when CCS runs the closing process at month end and is reviewed for reasonableness. David reconciles all capital asset types, including depreciation balances, between the AM and GL at year end. Periodically, he also performs testing of sampled assets to validate depreciation calculations.

## Key Controls:

**Key Control #1 (Manual: Existence / Valuation):** The Inventory Control Specialist adds asset information such as Profile ID and acquisition cost to the Asset Management Module in ctclink using source documentation such as invoices and receiving reports to ensure the system reflects an asset that actually exists and one that is appropriately valued.

**Key Control #2 (Automated: Valuation):** The College relies on the depreciation calculated by ctclink. The system automatically calculates depreciation based on the asset profile type and information entered: in-service date, commodity code, and asset value.

## Identified Weaknesses:

**None**

## **STEP 2: Confirm Key Controls**

**Key Control #1 (Manual: Existence / Valuation):** The Inventory Control Specialist adds asset information such as Profile ID and acquisition cost to the Asset Management Module in ctclink using source documentation such as invoices and receiving reports to ensure the system reflects an asset that actually exists and one that is appropriately valued.

To confirm this key control we reviewed *Voucher ID* 00047505 and *Invoice No. INV\_69119* for the asset "Anatomage Cadaver Table". We inspected the A/P module in ctclink that contained the PO information that was input by The Inventory Control Specialist and reviewed by Yabing Fisher, Senior Expense Accountant, that included asset information such as Profile ID, acquisition cost, and date. We noted that the

## State of Washington

"Invoice Total" field in ctcLink was \$91,560 added on 9/11/23. We reconciled this by reviewing the actual actual vendor invoice from "Anatomage Inc." for the total amount of \$91,560, with an invoice date of 9/11/23. We were able to confirm that the details entered from the original invoice matched the purchase order that was in ctcLink. ***No issues noted.***

**Key Control #2 (Automated: Valuation):** The College relies on the depreciation calculated by cTcLink. The system automatically calculates depreciation based on the asset profile type and information entered: in-service date, commodity code, and asset value.

The confirmation of this key control and the understanding of the related general IT control is documented at [[IT Control Testing - Depreciation](#)].

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* IT Control Testing - Depreciation

*Prepared By:* NJH, 10/2/2024

*Reviewed By:* RKM, 10/7/2024

Purpose/Conclusion:
---------------------

**Purpose:**

## State of Washington

To determine whether the College relies on the depreciation calculated by ctcLink and whether the system automatically calculates depreciation based on the asset profile type and information entered: in-service date, commodity code, and asset value (**key control #3 - Depreciable Capital Assets**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [[Depreciable Capital Assets - Controls](#)].

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

# State of Washington

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is*

## State of Washington

*controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:



# State of Washington

## Software Calculation:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

## **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **STEP 1: Understand Automated Key Control**

**Significant System:** Asset Management (AM) Module - ctcLink

**Key Automated Control:** The College relies on the depreciation calculated by ctcLink. The system automatically calculates depreciation based on the asset profile type and information entered: in-service date, commodity code, and asset value.

## State of Washington

Our understanding of the overall control is documented as part of our understanding of controls over relevant assertions for Asset Management at [\[Depreciable Capital Assets - Controls\]](#).

### **STEP 2: Confirm and Test Automated Key Control:**

See IT Control Testing at [\[Depreciable Assets Testing\]](#) on tab "IT Control Testing".

To confirm and test this key control, we haphazardly selected an asset that was a new FY24 addition placed in service during the fiscal year listed within the AM module provided to us by Tiffany Henderson, Dir. of Financial Reporting, on 9/17/24. We then re-performed depreciation calculations based on the listed useful life, cost, and acquisition date as listed in AM. We first analyzed the asset class and compared it with the useful lives listed in [SAAM 30.50](#). We noted no variances in useful life. We then recalculated monthly depreciation and A/D for all of the selected assets and compared these amounts with the A/D amount listed in AM. We noted no variances. From our testing, we are able to confirm that the automated control accurately calculated depreciation based on the in-service date, commodity code, and asset value and that it was in place during the current fiscal year. *No issues noted.*

### **STEP 3: Understand General IT Controls**

To gain an understanding of general IT controls, we met with Brandy Browning, Director of Budgeting and Account, who is the Subject Matter Expert (SME) for the Financial Management (FIN) pillar within ctcLink for CCS along with Stephanie Beaulieu, IT Customer & Services Manager, and Tiffany Henderson, Dir. of Financial Reporting, on 9/18/24. We inquired about how access is assigned to certain individuals and the process for allowing and changing user access roles within different modules of the ctcLink Pillars. Someone is first assigned access by a SME based on the users position, duties, and responsibilities within the college, who will then review if the user needs to have access to the specific pillar. When someone needs to access or make changes in a module or pillar of ctcLink that they were not originally given access to, they must first discuss this with their direct supervisor. If the supervisor agrees that an individual needs additional access, they will submit an internal IT help ticket requesting access to a certain module or pillar and will select from a drop-down menu from the list of applicable SME's at the college. This ticket will be sent to the IT team who then automatically routes it to the appropriate SME. The SME will then determine based on their knowledge of the pillar, business need case for access and qualitative factors based on experience, role, etc. to determine if the user should be given permission to access the pillar (**General IT Control #1**). Once decided, the SME will route the IT ticket back to the IT team on behalf of the original sender (user) and the IT team will correspondingly make the change on their end by updating the user access list within the respective ctcLink pillar/module. Both SME and IT personnel can run reports at any time to view who currently has access to which pillars/modules, and can identify and investigate any further changes that need to be made.

For the Asset Management module within the Financial pillar of ctcLink, we inquired about how the AM module determines the logic needed to run the necessary code that is responsible for calculating the depreciation based on other chart string user inputs by Yabing Fisher (Expense Senior Accountant) such as useful life, commodity code, etc. Stephanie informed us that if someone within the AM module identifies a potential issue, all module related code changes are processed by SBCTC through a separate help center online and will work with the user to address the issue via email updates about the ticket's status (**General IT Control #2**). SBCTC is responsible for managing the system level logic that runs on each

## State of Washington

module at all colleges using ctcLink, which is why no changes can be made from the IT team at the individual college level.

### **STEP 4: Confirm Key General IT Controls**

**Key General IT Control #1:** The SME will determine based on their knowledge of the pillar, business need case for access, and qualitative factors based on experience, role, etc. to determine if a user should be given permission to access the pillar.

To confirm this general IT control we obtained and inspected a copy of the user access list for the AM module as of 10/2/24. We noted only four individuals who have roles/access to the "ZZ AM Mass Transactions (N)". We were able to note that all users have current "@ccs.spokane.edu" email addresses, and only one user, Yabing Fisher, Expense Senior Accountant, has full access. The other individuals listed have read only, action, and correction actions available. We verified that there did not appear to be an unreasonable number of employees who have access to make full changes in the AM system. *No issues noted.*

**Key General IT Control #2:** If someone within the AM module identifies a potential issue, all module related code changes are processed by SBCTC through a separate help center online and will work with the user to address the issue via email updates about the ticket's status.

To confirm this general IT control we obtained and inspected a copy of an SBCTC service help desk ticket #181342 created on 11/30/23 by Yabing Figher, Expense Senior Accountant. We noted that the error was regarding an issue with the "Combo Edit Error" when trying to retire certain assets during month end close within the AM module. We then analyzed the thread of communication with Kim Cook, the assigned technician, and several other SBCTC IT technicians with Yabing and noted that the ticket was set to "resolved" as of 12/12/23 and was "closed" on that same day. *No issues noted.*

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* Depreciable Capital Assets - Testing

*Prepared By:* NJH, 10/4/2024

*Reviewed By:* RKM, 10/10/2024

Purpose/Conclusion:
---------------------

# State of Washington

## **Purpose:**

To determine whether reported capital assets represent real assets, as of the end of the period (Existence).

To determine whether capital assets are reported at properly valued and calculated amounts (Valuation).

## **Conclusion:**

We were able to determine that the reported capital assets represent real assets, as of the end of the period.

We were able to determine that the reported capital assets are reported at properly valued and calculated amounts.

## Testing Strategy:

The following is a list of **considerations** for testing the existence assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Nonexistent Assets**

Review capital asset records to determine whether records meet minimum requirements of BARS [3.3.9.40](#) to positively identify and adequately describe the asset. If asset records are not sufficient, follow up on how the entity is able to identify and track reported assets and consider further audit procedures.

Scan the capital asset list for unusual or unexpected assets or patterns.

*For example: asset descriptions that appear insufficient to identify the asset, asset descriptions that seem strange, assets with a historical cost that doesn't appear to meet the capital asset threshold, assets that are past the end of their service life, assets or asset types that don't appear to belong (based on auditor's understanding of entity activities and area of operation), assets or asset types that the auditor doesn't recognize, attributes that appear unreasonable (historical cost, useful life or scrap value), assets that appear connected to actions noted in planning procedures (impairment, replacement, sale or surplus, transfer), etc.*

Test sampled assets or selected high-risk assets from accounting records for existence by observing them or reviewing documentation.

*Observation for aboveground infrastructure such as roads, bridges or buildings may be by [google maps](#). Documentation for underground assets may consist of maps, system plans approved by regulatory agencies or permits, etc.*

Review the government's records of the latest physical inventory for any identification and follow-up on missing assets or any types of assets or locations that were not covered. Note: review of a government's physical inventory is considered a control test. However, it may be done as a risk assessment procedure to help direct substantive testing, and follow-up on results may result in some substantive evidence.

Trace assets from accounting records to assets listed on the government's insurance policy records. Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

## State of Washington

Trace assets from accounting records to operational records (ex: Public Works Department typically tracks assets for maintenance or regulatory reporting purposes). Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

For land and buildings, trace parcels and historical cost per the land subsidiary schedules to the County's land (GIS) records to verify ownership. Note: this test also provides evidence for the rights & obligations assertion and - if a complete list is obtained from the County - for the completeness assertion as well.

Compare reported public project completed or in process during the period to the L&I [prevailing wage reporting database](#). Note: since reporting is done by contractors, it would be considered a third-party verification of project existence. We would expect capitalized costs (which include costs incurred by the government as well as contractors) to exceed the contractor's reported costs for most projects. This test also provides evidence for the completeness assertion if traced from the L&I database.

### **Cut-off**

Review supporting documentation to verify dates of any transfers, annexations or donations.

See the Expenditures | Existence step for testing strategies on cut-off for capitalized expenditures.

### **Detail Roll-Up**

If manual journal entries are required to update the GL, agree figures per the GL to subsidiary schedules or systems.

Search for manual journal entries that debit (increase) capital or infrastructure assets. Consider testing if any risk indicators are noted.

Reconcile (or review the government's reconciliation) capital expenditures for governmental funds to increases in capital assets. The only anticipated reconciling item would be equipment that is below the capitalization threshold.

Reconcile (or review the government's reconciliation) increases in capital assets to capital purchases and sales per the statement of cash flows for proprietary funds. The only anticipated reconciling item would be donated or contributed assets.

**Over/Invalid Capitalization** - See classification step for testing strategies on improper capitalization upon construction or acquisition, or when determining whether an expense is a maintenance or repair expense or a capitalized improvement.

### **Unrecorded Disposals or Impairments**

Scan capital asset records for fully depreciated assets and inquire as to the status (disposed, no longer in use, etc.) to ensure all retirements and disposals have been recorded. Evaluate appropriate accounting for any fully depreciated assets remaining in service in accordance with [BARS 3.3.10.130](#).

Identify significant disposals, impairments (due to obsolescence or damage) or contributions per review of minutes and trace to asset records to verify these events were accounted for.

Request a list of insurance claims made during the audit period to identify possible impairments or removed assets, then trace to subsidiary records to verify that the event was properly accounted for.

## State of Washington

Identify annexations (through minutes, inquiry or OFM's central annexation tracking system) and trace to supporting documents showing the transfer of assets. Note: this test would also provide evidence for the completeness and rights & obligations assertions.

The following is a list of **considerations** for testing the valuation assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Incorrect Depreciation Calculations**

Perform an analytical review of depreciation expense by type of asset for reasonableness.

Re-calculate depreciation expense for a sample of assets or in conjunction with a test of automated controls (if depreciation is automatically calculated by the system). Consider testing the inputs used for the calculation to determine whether they are reasonable and in line with any applicable policies; i.e. useful life, salvage value, etc. Alternatively, test calculations, extensions and footing of subsidiary records if records are maintained on spreadsheets.

Evaluate capital asset policies for componentization or grouping of assets to determine if it has been consistently followed and will result in a rational method of depreciation. See BARS [3.3.10.150](#) for guidance.

Evaluate estimated useful life and scrap value factors for reasonableness. This test could be done in general (on the government's accounting policies), for selected asset classes or for selected or sampled asset records.

*If testing selected high risk assets, auditors should consider assets that are nearly or fully depreciated (see BARS [3.3.10.130](#)), assets with unusually high or low useful lives for their type, and assets with unusually high scrap values.*

Compare estimated useful lives for assets with replacement schedules / policies and capital budgets.

*We would expect that assets on a regular replacement schedule (such as equipment, vehicles, road surfacing, etc) or that are included for replacement in the capital budget would have estimated useful lives that match the government's replacement plans for the asset.*

Consider whether the date placed in service for assets is reasonable given when the asset begins being used or is substantially complete as this will have an effect on when depreciation begins. See information in BARS [3.3.10.90](#) about when to move a project out of CIP.

### **Impairment**

Check that the measurement method used for write-offs is in accordance with GAAP (GASB 42.12-15). Review or recalculate the portion of historical cost that should be written off for impaired capital assets. *Note: auditor would normally use the same measurement method used by the government unless it the auditor finds it inappropriate for the circumstances or unallowable under GAAP.*

### **Incorrect Historical Cost of Assets**

# State of Washington

Trace recorded cost to supporting documentation. *Note: This test would normally be limited to recent additions, since documentation for historical assets has likely passed the records retention period.*

Evaluate the reasonableness of any estimates of the historical cost of capital assets.

Evaluate the reasonableness and support for any estimates of the acquisition value (per GASB 72) of donated capital assets.

## Conversion to GAAP

For governments converting to GAAP reporting, examine valuation method for retroactively reported infrastructure assets and verify that the valuation method used is one of the methods prescribed by the County Road Advisory Board.

## Modified Approach

Check that infrastructure is being depreciated unless the modified approach is used. If the modified approach is used, verify that the government has met criteria of GASB 34 par 23-26.

## Allocation

On the government-wide statement of activities, review allocation of depreciation for capital assets for governmental funds. Depreciation expense will be reported as a component of the direct expense shown in the statement of activities. Request spreadsheet for allocation.

Guidance/Criteria:

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

GAAP criteria for reporting capital assets

[\*\*GASB Codification Section 1400 Reporting Capital Assets\*\*](#)

[\*\*GASB Comprehensive Implementation Guide Chapter 7 Basic Financial Statements and Management's Discussion and Analysis, sections 7.9-7.21\*\*](#)

Record of Work Done:

## **Significant Balance and Assertions:**

Governmental Activities - Depreciable Assets (Net of Accumulated Depreciation) - Existence, Valuation

Controls are documented at [[Depreciable Capital Assets - Controls](#)].

## **Auditor note on substantive testing for FY24:**



## State of Washington

Due to prior unresolved issues in prior audits regarding variances between the GL and data from Asset Management (AM) module in ctcLink, we performed an updated reconciliation between the two systems for FY24 to identify and determine which data set appeared to be more reliable to use for substantive testing purposes. We also met with Tiffany Henderson on 9/23/24 to address these concerns. From our updated understanding and data provided from our reconciliation, we have determined that substantive testing will rely on different aspects of each data set as it appears reliable to us based on qualitative and quantitative factors, and based on what data is available and needed for particular testing strategies. The following areas used from each data set are as follows:

### G/L Data:

- Additions samples
- Additions costs
- Additions placed in service date

### AM Data:

- Buildings (existence) beginning balance cost
- Buildings (existence) asset ID number
- Additions description, class life, accumulated depreciation

The variance between the GL and AM is shown in our reconciliation here [[Depreciable Assets Testing](#)] under the "*GL to AM Recon*" tab. We originally noted a NBV variance of \$23,751,018.75 between the two accounting systems. We addressed this issue with Tiffany Henderson on 9/23/24, whereby on 9/30/24, Yabing Fisher, Senior Expense Accountant, provided us with an updated and corrected reconciliation which noted a variance below the floor. Note that our substantive testing was already in process when the updated reconciliation was provided, and we relied on the original data provided. The variance did not impact our testing strategy or overall variances. ***No issues noted.***

### **Substantive tests performed to meet the Existence assertion:**

See substantive testing at [[Depreciable Assets Testing](#)].

### Additions:

To test the existence assertion for FY24 asset additions, we selected a sample of new assets placed in service during the FY from the G/L by identifying journal ID's with "Add" in the description. We then used the sampling spreadsheet with a tolerable misstatement set at 7.5% and the assurance set at moderate to have a sample size of 10 assets. We then used the following testing attributes on each of the selected assets in our sample:

D - There was appropriate supporting documentation via invoices, receipts, or purchase orders to verify the asset addition existed.

We noted no variances or exceptions during our substantive testing. We are able to determine that the reported capital represent real assets.

# State of Washington

*No issues noted.*

## **Substantive tests performed to meet the Valuation assertion:**

### **Additions:**

To test the valuation assertion for FY24 asset additions, we selected a sample of new assets placed in service during the FY from the G/L by identifying journal ID's with "Add" in the description. We then used the sampling spreadsheet with a tolerable misstatement set at 7.5% and the assurance set at moderate to have a sample size of 10 assets. We then used the following testing attributes on each of the selected assets in our sample:

- A - Auditor recalculation of accumulated depreciation does not deviate from system calculated depreciation.
- B - The historical cost of the asset ties to supporting documentation including all costs as mentioned in GASB Codification 1400.
- C - The asset SAAM life is reasonable and consistent with the assets' description and the nature of the asset.

We noted an overall variance below the floor and no issues during testing. We were able to determine that the reported capital assets are reported at properly valued and calculated amounts. *No issues noted.*

## **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* Charges for Services - Controls

*Prepared By:* JAG, 10/7/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion.*
----------------------

### **Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

### **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive

# State of Washington

testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**This workpaper template was designed for tuition revenue system control audits at Community Colleges. Contact [Team IT Audit](#) with questions on information or steps contained in this template. The template assumes occurrence and valuation are relevant assertions and that controls over occurrence and valuation will be tested.**

The following procedures are **required** for all relevant systems:

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption [RCW 42.56.420](#) for cyber security purposes. The details documented in the record of work and supporting workpapers may qualify for this exemption. Auditors must include this statement in workpapers: "**This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited**".

## **STEP 1: Control Understanding**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*See the **Client Resource Tab** to reference query tools and year end adjustment information applicable to community and technical colleges. The following are expected controls for and community technical colleges. If sufficient key controls are not in place, the government may be able to demonstrate compensating controls.*

*Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of COSO elements as documented in the "Entity-wide COSO Evaluation" step as they relate to this particular system.*

When gaining an understanding of a college's tuition revenue system, the following specific steps should be considered:

### **Admissions & Class Registration**

Discuss admissions and class registration procedures with department representatives or registrars to gain an understanding of admissions and registration processes and policies. Consider the following:

## State of Washington

How is a student's status validated?

How do they assure that a student's status has been accurately posted from Campus Solutions Core to Student Finance (SF)?

### Tuition calculation

The automated tuition calculation processed in the cTcLink system has been identified as an automated control. When gaining an understanding of a college's software calculation controls, the following specific steps should be considered:

Gain an understanding of the college's procedures for updating Term Fees, Tuition Groups, Item Types, and Tuition Schedule tables, including any review they perform to ensure the changes made are correct.

Validation of Tuition Calculation at the College - Inquire with college staff to see if they test tuition calculations prior to rolling over term fees, and if so, whether they used the Production College Development (PCD) environment to do so. If they have saved supporting documentation for testing performed, observe testing results to verify that the respective tuition and fee values were actually calculated correctly for each category of mock student tested.

Identify individuals responsible for updating the tuition rates including any users who are authorized to modify the tables or access the screens which have been deemed critical to the tuition revenue calculation process (Term Fees, Tuition Groups, Tuition Calculation, Item Types, and Tuition Schedule)

Consider obtaining the following from college staff when testing calculation of tuition revenue for a sample students:

Approved tuition rates

**Customer Account** reports showing tuition/fee charges on the student accounts

**Customer Academic Information** and **Career Term** data showing the student's status/tuition group

**Enrollment Summary** showing evidence of the classes the student was enrolled in for the selected quarter.

### Tuition payment

Students typically pay tuition and fees by credit card. Credit cards are processed through CyberSource. State and community technical colleges must reconcile payments received, and each individual college establishes their own frequency to complete it. Each cashier closes out daily using a batch report from the cTcLink system. The daily batch report may not include daily transactions for EFT's and wires. The following steps should be considered when gaining an understanding of tuition payment:

Discuss cash receipting procedures with department staff and document procedures performed tuition payments paid with the following

Cash or check

Credit Card

ACH/Wire

## State of Washington

We expect colleges reconcile credit card payments made through CyberSource. Inquire and document the colleges process of tying credit card payments processed through CyberSource to entries made in the cTcLink system.

Inquire regarding how the college would address variances found when performing reconciliations.

### Posting to the GL

Receipts are posted to the GL through an evening automated batch process. Typically, cash receipts are reconciled daily to bank accounts, and bank account balances reconciled monthly to cTcLink. Consider the following:

Gain an understanding of the GL posting process, and determine how they validate that their postings are accurate and complete.

Inquire regarding how the college would know if the GL did not post accurately or completely. It is likely there will be variances in how each college performs their reconciliations, with some using spreadsheets or running queries or customized reports as tools to validate the GL postings.

### Distribution / Allocation to Revenue accounts

Review the procedures the college uses to assure that all tuition revenue payments from GL fund 840 were completely distributed. Consider the following:

Document the process used by the colleges to update/maintain the values in their Tuition Distribution table.

### Transfer to AFRS

Gain an understanding the college's reconciliation process of their cTcLink balances to those posted to AFRS. Consider the following:

Evaluate the college's procedures regarding the year-end closing entries recommended by the State Board (per their "Year End Closing" binder). While the key control is the reconciliation done by the SBCTC, the college still needs to provide oversight and monitoring of the adjustments that are recommended by the SBCTC (colleges should understand what the adjustments are for, that they are correct and properly supported).

*Note:* SBCTC System Accounting Coordinators handle all ctcLink uploads to AFRS. Every month, on AFRS cutoff date, a staff from SBCTC runs a query in ctcLink of all journal entries created. This is a summary level report that is downloaded into an Excel spreadsheet. Staff create two pivot tables; one by funds and amounts, another by general ledgers and amounts. Staff expects the pivot table by fund and amount to be zero. Staff then compares the second pivot table to another report, which is generated for the State Auditor's Office (SAO). Both reports are queried from the same database, the one for SAO contains a few more fields. When all the amounts agree, staff is ready to prepare the file to be uploaded into AFRS.

Staff then sort the file by fund, general ledger, and amount. The customization now generates the output files (flat files with transaction codes) and sends them to AFRS. There are usually 1600 to 2200 lines for each college each month. This file is saved as a flat file format and is uploaded into AFRS using the OFM's Financial Toolbox. Sue does a test run in what is known as the SUP

## State of Washington

environment (copy of previous day's production) to check for any major issues. Staff is able to capture a copy of the flat file and uses that to reconcile between what is in cTcLink and what was transmitted to AFRS. Staff makes any necessary corrections to the AFRS batch and releases the output file to AFRS.

Financial Adjusting Entries – the colleges are directed to use the adjusting entry forms to enter any required cTcLink adjustments, with each suggested adjusting entry denoted in this section. Additional explanations (from the SMARTER system) for each of the suggested adjusting entries are also provided.

SMARTER Queries used to reconcile Finance Sub Modules to the General Ledger. Not all State community and technical colleges use SMARTER Queries, however, use is encouraged by SBCTC.

*Note: Waivers are not included in data reported from cTcLink to AFRS*

Disclosure Forms – Copies of the college's general note disclosures and supporting documentation.

Payable/Receivable reporting reflecting any payables ("due to") and receivable ("due from") transactions with other state agencies.

*Note: Some reports and queries used by colleges may be built in-house and may be used alongside SMARTER queries that have been built by SBCTC. If the college does not have a good understanding of the reconciliation process done by the SBCTC then the auditor may want to consider reviewing the year-end adjustments for material errors. For example, the auditor could request the Year End Closing documentation from the State community or technical college and review it to determine the types of adjusting entries and exception items noted by SBCTC.*

### **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

### **Step 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4.A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.*

### **STEP 4: Test Controls**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were*

## State of Washington

*consistently and effectively applied).*

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

***Since key controls for Tuition Revenue are automated, Auditors should add the "IT Control Testing - Tuition Calculation" step available in the Store to document automated and general control testing.***

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of COSO elements. In doing so, all of the following specific determinations must be documented:*

- A. Key controls – including personnel who affect the application of the control – have not changed since they were last tested. Automated controls should be tested the first year that colleges use the cTclink system.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2021, this work could potentially be relied upon for both the periods ending 2022 and 2023.*

### **Step 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

## **SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Education - Higher Education Charges for Services - Occurrence, Valuation  
Higher Education Special Revenue - Charges for Services - Occurrence, Valuation

See lead sheet here: [[Lead Sheet](#)]

## **STEP 1: Gain an Understanding of Internal Controls**

On 9/17/24, we met with Tiffany Henderson (Director of Financial Reporting), and Diana Plum (Student Finance Accounting Manager), to gain an understanding of controls over Charges for Services.

Software used by community colleges to generate tuition revenue is developed and maintained by State Board of Community and Technical Colleges (SBCTC). Student information is captured in the ctcLink system, within the Campus Solutions Core module (CS). Tuition is automatically calculated and applied to student accounts within the Student Financials module (SF). The rates and codes used in the tuition calculation process reside within several key system tables, which are maintained in part by SBCTC, and by the local colleges.

## **Admissions & Class Registration**

Students can register on-line at the Admissions office, where the student application is processed within the CS module. Critical information associated with tuition revenue is captured at this point regarding the student's status (i.e. resident, non-resident, veteran, etc.), and this data is then posted to CS. When the first billing record is generated for the student (i.e., for admissions or testing fees), a billing account is then created for the student in CS.

Students typically register for classes on-line, but they can also do so in person. Classes are defined within CS. The information captured in CS during registration is then used in calculating the amount of tuition owed by each student. (i.e., residency, waiver, and credit load information is



# State of Washington

used in conjunction with rates defined in the SF tuition tables, to generate an owed tuition amount).

A student's tuition and fee liability is recorded in the Campus Solutions Core database when students register for classes, but revenue will not be recognized in the GL until a journal is created in CS and sent to SF via nightly batch.

## **Tuition and Fees Calculation**

Tuition and fees are automatically calculated by the ctcLink system (**Key Control 1 - Valuation**), based on the following factors:

- Residency - in state versus out of state rates, student status as determined by student assertion and FAFSA information.

- Division - rates vary for lower (freshman and sophomore) versus upper (junior and senior) level classes.

- Credit Load - a student's amount of registered credits, as determined by their registration schedule within the CS module.

- Waivers or Special Programs - there are a plethora of tuition waivers which students may qualify for, such as 'children or spouses of deceased or disabled law enforcement officers/firefighters', and 'high school completion'. There are also available programs such as 'Running Start'.

These programs and waivers reduce or completely waive the overall tuition amount owed by the student.

We performed IT Control testing of this automated calculation at the IT Control Testing step here: [[IT Control Testing - Charges for Services](#)]

## **Tuition Payment**

Tuition can be paid on-line or in person at the Cashier's office. Payments are captured by the ctcLink receipting module and recorded Student Financials (SF). Each college may use a tuition installment program allowing designated students to pay tuition in several installments.

Outstanding balances are retained only in Student Financials (SF) and posted to the GL when payment is made.

### **Cash**

There are always two staff (cashiers) in a cash receipting location. When cash is receipted, funds are immediately counted by a cashier, who then processes the posting of the payment to the student's account, and provides a receipt. The cashier also stamps checks for endorsement. Cashiers keep endorsement stamps and deposit-ready material in a safe. Access to the safe combination is restricted to necessary individuals, and is granted by internal audit. Cash which is received throughout the day remains in a locked till. At the end of day, the till is balanced and reconciled. Each cashier is responsible for their own reconciliation. The reconciliation process includes comparing receipts from the credit card terminal and cash in the till to the ctcLink 'review tender' screen within the cashiering module. Once these amounts balance, the cashier completes an Excel tracking document and prints this document. At this point, each cashier reviews, counts, verifies, and signs off on each other's work. All cashiering documentation backup (the Excel tracker, 'review tender' screen information, and receipts) are bundled and retained. Deposit-ready cash items are placed in the safe to await secure transport. Loomis Security Transport trucks come and pick up funds 3x a week.

### **Online Credit Card Payments**

Payments made through CyberSource are automatically linked into system (online credit card payments). CyberSource automatically posts to ctcLink, which flows through to the GL via the SF journal (posted in a daily SF batch).

# State of Washington

## ACH/Wire Transfer

This payment method is mainly used by international students. The software 'PayMyTuition' is utilized, which functions similarly to CyberSource. A confirmation of the wire is provided to CCS, and once funds are received, CCS manually inputs the payments into ctcLink.

## Payment Plans

Nelnet offers a payment plan which spreads the total payment amount for a term in equal installments over the length of the term. Students who wish to enroll may elect to do so within 30 days of term start. Similarly to CyberSource, Nelnet payments are automatically linked into the system as they are received.

Laurice May (Fiscal Analyst 2) performs a daily bank reconciliation to ctcLink, by running an electronic data download from the Bank of America, and reviewing each individual transaction, tying it to the ctcLink journals. Variances are investigated, corrected, and communicated up to Clint (Fiscal Services Account Manager), and then to Tiffany. At month end, Laurice performs the bank statement to GL activity reconciliation for all cash counts. Typically, there are multiple bank activities that need to be reconciled.

CCS has found that reconciling the journals by type has helped them to complete more accurate bank reconciliations. After Laurice prepares the reconciliation then Clint (Fiscal Services Account Manager) reviews and approves it to ensure accuracy (**Key Control 2 - Occurrence**). At year-end, a similar process is performed as with month end.

## **Scholarship Allowance/Tuition Discount**

We received the 'Scholarship Allowance Calculation FY 2024' spreadsheet from Tiffany Henderson, detailing the steps to calculate the amount to reduce scholarship expense. The college computes the total postings to students' accounts receivable that could potentially generate a refund and then they compute the proportion of institutional resources that represent scholarship allowances and student aid expenses that could generate a refund. Next they compute the amount of scholarship allowances and lastly calculate amount by which to reduce scholarship expense by taking the total scholarship allowance per NACUBO calculation, less tuition waivers already booked as a reduction of tuition, less housing room waivers netted against auxiliary revenue. The estimate of the amount to reduce scholarship expense for FY24 is \$5,000,000.

## **Posting to the GL**

Tuition revenue is recognized when a student's enrollment is complete and student status is validated. Upon completion of the student's enrollment, a journal entry is created in Campus Solutions Core and sent to Finance via nightly an automated nightly batch process.

Cash receipts are posted to the GL through a nightly batch process, and if there are posting problems, the system notifies the user that the batch did not post. Corrections are made through a batch edit screen and the corrected batch is remitted. Tuition payments result in revenue being posted to Fund 840 under the source codes 0424 (tuition) and 0430 & 0431 (supplemental fees). Note that Spring/Summer pre-payments for Fall Quarter tuition are posted to GL account 5192 (deferred revenue).

## State of Washington

In order to validate that GL postings are accurate and complete, CCS has designated Clint McGregor (Fiscal Services Accounting Manager), as responsible for a daily check of which system generated journal entries (as described above) were generated during overnight processing. He reviews these journal entries that will post automatically as long as there are no errors. Part of Clint's review includes ensuring that expenses can be covered by a valid budget within the system and that revenues are expected (**Key Control 2 - Occurrence**). For custom journal entries, Clint is the first reviewer, and Tiffany is the second. Custom journal entries are denoted by a 000 prefix. Custom journal entries are required to include backup attachment information explaining the purpose of the journal entry.

To additionally ensure completeness and accuracy, system-generated GLs are set up to not allow any adjustments. For custom journal entries, in addition to undergoing multiple rounds of review, the person who requested the entry will also re-run data after the adjustment is made, functioning as a third level of review.

### **Distribution / Allocation to Revenue accounts**

An automated monthly process is run in ctcLink to allocate tuition revenue payments from GL fund 840 to the funds below. With the exception of Service & Activities fees (set by the Local Board of Trustees), the individual fund distribution percentages are determined by the Legislature. The local college manually posts and retains these percentages in the Tuition Schedule.

- 060 (Building fee portion; remitted back to the State)
- 149 (Operating fee portion)
- 522 (Services & Activities portion)
- 561 (Comm/Tech College Innovation portion)
- 860 (Institutional Financial Aid portion)

We obtained the tuition and fee schedule from Tiffany as part of our PBC requests at the start of the audit.

### **Transfer to AFRS**

The process continues to be a manual, although SBCTC is working on an automated interface to transfer financial data to AFRS. System Accounting Coordinator handles all ctcLink uploads to AFRS. Every month, on the AFRS cutoff date, runs a query in ctcLink of all journal entries created. This is a summary level report that is downloaded into an Excel spreadsheet. The Coordinator then creates two pivot tables; one by funds and amounts, another by general ledgers and amounts. Staff expects the pivot table by fund and amount to be zero. Staff then compare the second pivot table to another report, which is generated for the State Auditor's Office (SAO). Both reports are queried from the same database, the one for SAO contains a few more fields. When all the amounts agree, staff prepare the file to be uploaded into AFRS.

Staff then sorts the file by fund, general ledger, and amount. The customization now generates the output files (flat files with transaction codes) and sends them to AFRS similar to how it is done in the Legacy system. There are usually 1600 to 2200 lines for each college each month. This

## State of Washington

file is saved as a flat file format and is uploaded into AFRS using the OFM's Financial Toolbox. A test run in what is known as the SUP environment (copy of previous day's production) is then used to check for any major issues. Staff is then able to capture a copy of the flat file and uses that to reconcile between what is in ctcLink and what was transmitted to AFRS. Staff makes any necessary corrections to the AFRS batch and releases the output file to AFRS.

In addition to the SBCTC-provided checklists and steps listed above, CCS follows their own internal check list at year-end close. The checklist assigns various staff members responsibilities for making end of year closing entries. Tiffany Henderson and Brandy (Budget Director) review all year-end closing work.

### **Key Controls:**

**Key Control #1 (AUTOMATED - Valuation):** The ctcLink system automatically calculates tuition and fees for all students based on residency, division, and credit load status.

**Key Control #2 (Occurrence):** Cash receipt records are reconciled to electronic bank statements on a daily basis, and the bank statements are reconciled to GL activity on a monthly basis, ensuring reported revenue activity occurred in the correct period. This reconciliation is prepared by the Fiscal Analyst 2, and reviewed and approved by the Fiscal Services Account Manager. Financial Reporting staff reviews the system-generated journal entries, ensuring they are accurate and complete.

### **Identified Weaknesses:**

**None.**

### **STEP 2: Confirm Key Controls**

**Key Control #1 (AUTOMATED - Valuation):** The ctcLink system automatically calculates tuition and fees for all students based on residency, division, and credit load status.

The confirmation of this key control and the understanding of the related general IT control is documented at: [[IT Control Testing - Charges for Services](#)]

**Key Control #2 (Occurrence):** Cash receipt records are reconciled to electronic bank statements on a daily basis, and the bank statements are reconciled to GL activity on a monthly basis, ensuring reported revenue activity occurred in the correct period. This reconciliation is prepared by the Fiscal Analyst 2, and reviewed and approved by the Fiscal Services Account Manager. Financial Reporting staff reviews the system-generated journal entries, ensuring they are accurate and complete.

We reviewed the June 2024 reconciliations for each bank account and noted that each one was prepared by Laurice May and approved by Clint McGregor except for the Bank of America checking that was prepared by Clint McGregor and approved by Tiffany Henderson. See our detailed confirmation of bank reconciliation understanding at the 'Cash and Pooled Investment - Controls' program step at [[Cash and Pooled Investments - Controls](#)]. We also reviewed screenshots of a system-generated journal entry from 10/2/2024 and noted that Clint reviewed the

## State of Washington

transactional data to ensure it made sense and was accurate. We also noted a "P" under journal status showing the journal was posted and that it is valid meaning all of the chart strings balance. **No issues noted.**

### **STEP 3: Preliminary Control Risk Assessment**

**MAX - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.**

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.**

### **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* IT Control Testing - Charges for Services

*Prepared By:* JAG, 10/16/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion:

#### **Purpose:**

To determine whether the ctcLink SF module automatically calculates tuition and fees for all students based on student profiles (residency, division, and credit load) **(key control #1 - Charges for Services)** was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently

## State of Washington

during the audit period. However, we did not test the operating effectiveness of general IT controls.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Charges for Services - Controls\]](#)

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

#### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

#### **Automated Interfaces:**

Is data transferred in real time (immediately) or in a batch? If batched, how often does the interface occur (daily, monthly, quarterly, etc.)?

What triggers the data transfer?

*Transfers could be manually initiated, could be hardcoded into either the sending or receiving system's programming, could be controlled by administrative menus (for integrated software modules), or could be run as automated jobs with third party software or programming.*

Could the interface process fail? If so, how would the entity recognize that the process failed?

## State of Washington

*This may not be a relevant risk for integrated software, but may be the case for custom interfaces designed outside the software which may be subject to various points of failure.*

Will the interface process reject transactions or batches with errors? If so, who monitors rejections and follows up on rejected transactions to ensure correction (either in the sending or receiving systems) and how are corrections tracked and monitored?

*For example, information that could trigger a rejection or isolated transaction and batch can include: invalid data, duplicate data, or missing factors. If errors are possible, we would expect the isolated data is reviewed, tracked and corrected in a timely manner.*

Are any reconciliations done to provide assurance that data transfer was complete and accurate?

*We would expect the local government to perform a reconciliation between source and destination systems to ensure the interfaced data is complete and accurate. This may be a manual reconciliation or spot-check, a system or dashboard report, or automated edit check. Depending on how often errors (if any) are expected, the reconciliation could be done each time the interface occurs, or on a monitoring basis, like annually.*

### Edit Checks:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

## State of Washington

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### Computer Generated Reports:

What information or exceptions is the report designed to identify (what is the purpose of the report)?

How is the report used and by whom?

For exception reports, who reviews the report and how do they follow up on exceptions?

*Auditors should consider whether the exception report reviewer has appropriate authority and information to effectively follow-up on report results. For fraud-related risks, also consider whether the review position is appropriately segregated from positions that can initiate transactions. For exception reports that regularly identify many transactions needing multi-step follow-up, the manual review and follow-up may be identified as a separate key control rather than documented and evaluated as an aspect of the automated exception report control.*

What are the report parameters or criteria? Does the report have any calculated fields? If so, what are the calculations?

*The ideal method of documenting an understanding of a computer generated report is to get a screenshot or printout of the report parameters. If using a report writer, this may be printed with the report, or may be accessed from a design view or intermediary screen. For custom or complex reports, this may be the SQL code.*

*For exception reports, auditors should pay special attention to the definition of an exception embodied in the report parameters.*

*NOTE: observation of the report parameters will also count as a confirmation of the report and could also be used to test the report.*

### Electronic Approvals:

Inquire if the entity has a written policy or documentation describing the approval process and protocols for reviewers?

What is the approval process in the application?

What transactions, data, tasks, or documents are approved?

Who are the preparers? How do preparers submit for approval?



## State of Washington

Who are the authorized approvers? Are there backup approvers?

What documents or information are required to make approval judgment?

What is the next step once a transaction/data/ task/document is approved or denied?

Is there any exception situations where approval can be by-passed or waived?

Can the approver make changes to information during the approval stage? If so, is the preparer notified of the changes?

Can anyone make changes to the approved information after the approval stage? If so, are changes captured in an audit trail and is the audit trail (log) regularly reviewed and monitored to detect any unauthorized changes?

Does the application prevent users from approving their own work (self-approval)?

*Some applications have a feature preventing self-approval. If an application does not have a feature preventing self-approval, we would expect manual controls in place to ensure the segregation of duties between preparer and approver, if relevant to the risk.*

Does the application have high-level users that can also approve?

*High-Level Users (aka Users with elevated privileges, system or application "Administrators", "Super Users", etc.) typically have full access to change system settings and may have extensive function rights of software applications. Depending on entity's size and complexity, different high-level users may be responsible for the network vs. application level. High-level users represent a heightened risk for overriding segregation of duties and normal control processes.*

*We would expect entities to have compensating monitoring controls if personnel are responsible for both application settings and transaction processing controls.*

### **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

#### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

## State of Washington

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### Automated Interfaces:

Re-perform a reconciliation, comparison or analytical procedure between both systems to determine whether data interfaced completely and accurately. Alternatively, review the entity's reconciliation or comparison if they perform one.

*For example, auditors could perform count totals and summarize the data to determine whether the same number of transactions reside in both systems, or the total amount from the sending system was posted to the receiving system. Whether this takes the form of a comparison (numbers expected to match exactly), reconciliation (when reconciling items are expected) or analytical procedure (if numerous adjustments or reconciling items are expected) will depend on the nature of the interface and client documentation.*

*Note: these procedures would also provide substantive evidence.*

Observe documentation, such as interface logs or email notifications, to determine whether interfaces complete per expected interval (daily, monthly, quarterly, etc.).

*We would expect the data transfer to be consistent based on the programmed schedule. If data is expected to be transferred on a weekly basis, we would expect to see some form of documentation showing the weekly transfer.*

Observe evidence that batch jobs are monitored such as tracking spreadsheets or emails.

When interfaces did not occur as expected, determine whether procedures were followed to resubmit job or that there was a logical reason no data was received/sent for the interval (for example, it was a holiday so there was no interface for that day).

### Edit Checks:

Re-perform the edit check for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the check. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's*

# State of Washington

*testing procedures).*

*In some cases, it may be possible for the auditor to reperform the edit check for the entire population.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. Analytical procedures would normally also count as a substantive test.

## **Computer Generated Reports:**

For exception reports, inquire with the person assigned to review the report how frequently exceptions are noted by the report. Trace identified exceptions to documentation of correction or resolution.

Re-perform the report by either (a) generating it yourself in the entity's system (if the auditor has direct access to the system), (b) recreating the report using CAATS, or (c) by observing the report be generated in your presence. If observing, note any user-entered values or parameters and determine whether entered parameters were appropriate. Compare re-performed report to the one being tested.

## **Electronic Approvals:**

Observe a transaction to see the approval process and verify any key aspects of the process or limits.

If transaction data or reports include approval information, use CAATS to confirm that all transactions met authorization rules.

## **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

## State of Washington

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Automated Interfaces:

Inquire if the entity has experienced any errors or irregularities with the interface. Also how often changes are made to the interface, and how many changes (if any) were made during the year.

What are the procedures to authorize and make changes to the interface?

*Except for the most simple situations, we would normally expect update procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

## State of Washington

*If the data transfer is already going to be checked or reconciled, then there may be less need for specific test procedures on program changes since any errors will be identified right away.*

How are program changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

*If the program is controlled by a third-party, we would expect a process between the government and vendor that allows the government to make requests and receive communication at the completion of the request.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the system processes the interfaced data, but they may be responsible for working the interface error queues and reconciling the interfaced data.*

### Edit Checks:

Inquire if the entity has experienced any errors or irregularities with the edit checks. Also how often changes are made to the checks, and how many changes (if any) were made during the year.

How can the edit check be changed or customized?

*Edit checks may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

*In other cases, edit checks may be established or configured through one or more administrative menus.*

What are the procedures to authorize and make program changes or configuration/setting changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

## State of Washington

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the edit check, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### Computer Generated Reports:

Inquire if the entity has experienced any errors or irregularities with the report. Also how often changes are made to the report, and how many changes (if any) were made during the year.

How is the report triggered or initiated?

*For reports that are automatically triggered, the auditor would normally not identify job scheduling or monitoring as a general control since we would expect failure of the report to generate*

Is the report hardcoded into the program, or is it a custom or ad hoc report? Also, what manual inputs (if any) are required to run the report?

*What parameters, criteria (date ranges, fund number, departments) or instructions are entered by the user to generate the exception report. The more options entity personnel have to customize or modify the report, the higher the risk of human error and inaccurate or incomplete reports. Pre-programmed reports provide less flexibility than ad-hoc reports; however, if program change controls are in place, they are more consistent.*

## State of Washington

If the report is hardcoded into the system, how are program changes made?

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change vendor developed reports, but they may be responsible for triggering, setting certain parameters, and/or following up on exception report results.*

NOTE: if the auditor cannot identify sufficiently effective general IT controls, the automated control will need to be tested using the same methods as a manual control (ie: sampling throughout the period). For example, if the report is manually generated and highly dependent on a number of manual inputs each time, or if the report does not have formal change controls, such as an ad hoc report or excel-based report. In such cases, the automated report is controlled by limited access and the judgment of the report writer – that is, while the report is an automated component, there is also an integrated manual component to the control.

### Electronic Approvals:

How are users assigned preparer and approver roles? Are user accounts periodically checked for needed changes? See the [User Access](#) step in the Accountability folder for more control considerations.

If configurations or settings relevant to the approval process are controlled by an admin menu, who has access to this menu?

If the entity has access to source coding for approval controls, what are the procedures to authorize and make program changes?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to vendor developed/supported coding that controls how the electronic approval works, but they may be responsible for approval configurations or settings and/or user account management.*

# State of Washington

## **STEP**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

## **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the **SOC Report Reliance** workpaper in the Store.

### **Automated Interfaces:**

Review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, reconciling or comparing the data transfer (or reviewing the entity's reconciliation or comparison) may also provide this evidence if tests address all states of the interface during the period.

Inspect job processing error logs/reports. Observe evidence that errors in processing were isolated and resolved. For example, select a sample of rejected transactions and observe evidence to determine whether errors were appropriately corrected and the corrections were timely.



## State of Washington

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Edit Checks:

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the edit check may also provide this evidence if the re-performance tests address all states of the edit check during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Computer Generated Reports:

If the report is subject to program change controls (either due to being hardcoded or by being automatically triggered), review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

If the report is subject to program change controls, review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the report may also provide this evidence if the re-performance tests address all states of the report during the period.

If the report relies on manual inputs and report copies saved show the parameters entered, the auditor can check a selection or sample of reports to confirm that the report was run correctly.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### Electronic Approvals:

Review user access report to verify that current users are appropriate. Also consider review of user access change logs (if available) to evaluate user account management throughout the period. See the User Access step in the Accountability folder for more testing considerations.

## State of Washington

If approvals are governed by significant settings/configurations, and such changes are logged, review the change log to verify the population of changes for the year.

*Verification that no configuration changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity has access to source code, review the change log to verify the population of changes for the year. Then review programming change documentation or the entity's test documentation for selected or sampled changes.

*Verification that no program changes were made, along with the auditor's evaluation that no such changes are expected, would normally be sufficient evidence to conclude that no further testing is necessary.*

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the SOC Report Reliance worksheet in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the

# State of Washington

record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

## **Manual vs. Automated Interfaces**

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

## State of Washington

An “automated interface” is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered “manual” since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient’s age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient’s name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or

## State of Washington

may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

- Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined.

- Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

# State of Washington

## Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards [AU-C 315](#) Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards [AU-C 330](#) Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **STEP 1: Understand Automated Key Control**

**Significant System:** ctcLink Tuition Revenue System (Campus Solutions Student Finance module)

**Key Automated Control:** The ctcLink SF module automatically calculates tuition and fees for all students based on student profiles (residency, division, and credit load) and tabled tuition information (Valuation).

Our understanding of the automated control is documented as part of our overall understanding of controls over relevant assertions for Charges for Services at: [[Charges for Services - Controls](#)].

The tuition revenue calculation processing resides within a third-party vendor application system, which cannot be modified by system users. The only way for college users to affect the calculation is through edits to associated data tables and screens, and at the College-level, many of those tables are restricted to modification by the State Board.

# State of Washington

## **STEP 2: Confirm and Test Automated Key Control:**

We confirmed and tested the key automated control as follows, to determine whether the automated controls can be relied upon:

To confirm and test the automated control we recalculated the ctcLink calculated student tuition & fees amounts on student accounts. See tab 'Recalculation': [[Charges for Services Testing](#)]. We performed a recalculation of the student tuition and fees amounts billed to student accounts based on credit load, residency status, and division, and we noted no variances. From this testing, we are able to confirm that the automated control accurately calculated tuition based on student profiles and tabled tuition information, and that it was in place during the current fiscal year. *No issues noted.*

## **STEP 3: Understand General IT Controls**

To gain an understanding of general IT controls, we met with Brandy Browning, Director of Budgeting and Account, who is the Subject Matter Expert (SME) for the Financial Management (FIN) pillar within ctcLink for CCS along with Stephanie Beaulieu, IT Customer & Services Manager, and Tiffany Henderson, Dir. of Financial Reporting, on 9/18/24. We inquired about how access is assigned to certain individuals and the process for allowing and changing user access roles within different modules of the ctcLink Pillars. Someone is first assigned access by an SME based on the users position, duties, and responsibilities within the college, who will then review if the user needs to have access to the specific pillar. When someone needs to access or make changes in a module or pillar of ctcLink that they were not originally given access to, they must first discuss this with their direct supervisor. If the supervisor agrees that an individual needs additional access, they will submit an internal IT help ticket requesting access to a certain module or pillar, and will select from a drop-down menu from the list of applicable SME's at the college. This ticket will be sent to the IT team who then automatically routes it to the appropriate SME. The SME will then determine based on their knowledge of the pillar, business need case for access, and qualitative factors based on experience, role, etc. to determine if the user should be given permission to access the pillar (**General IT Control #1**). Once decided, the SME will route the IT ticket back to the IT team on behalf of the original sender (user) and the IT team will correspondingly make the change on their end by updating the user access list within the respective ctcLink pillar/module. Both SME's and IT personnel can run reports at any time to view who currently has access to which pillars/modules, and can identify and investigate any further changes that need to be made.

Tuition rates and fees are calculated based on information in Tuition Tables. The majority of these tables are maintained by SBCTC. For those tables and screens which are subject to CCS Board of Trustees (BOT) approval, the SF Accounting Manager (Diana Plum) is responsible for updating tuition and fee table rate information within ctcLink as necessary, as determined by BOT action. There are two types of rate tables that need to be updated and manually reviewed; SBCTC tuition rates and college specific fees. SBCTC updates the statewide tuition and required fees for students each year. The college specific fees may get updated on an annual and term basis. At the end of the year, the departments work together to determine if fees or charges need to change (increase or decrease), or add any new charges. These fees include the College wide charges such as the technology fee charged to every student, and course specific fees.

After it is determined that fees need to be adjusted, Scott, Program Specialist 3, and Holly, Instructional Service Manager, make the changes for the colleges. Once the adjustments to the fees are made, Tiffany, Director of Financial Reporting and staff in the Business office will pull a report

## State of Washington

to review these changes to ensure they are correctly implemented. After each update to tuition table rate information, the SF Accounting Manager haphazardly selects small samples of students and performs a re-calculation, to ensure that the ctcLink auto-calculation is functioning correctly (**General IT Control #2**).

### **STEP 4: Confirm Key General IT Controls**

**Key General IT Control #1:** The SME will determine based on their knowledge of the pillar, business need case for access, and qualitative factors based on experience, role, etc. to determine if the user should be given permission to access the pillar.

To confirm this general IT control we obtained and inspected a copy of the user access list for the SF module as of 10/7/24. We noted there are many individuals that have viewing acces to the SF module but only 14 individuals have access to edit tuition and fees. Their role access is titled 'SF Tuition and Fees Update'. We were able to note that all users have current "@ccs.spokane.edu" email addresses. We verified that there did not appear to be an unreasonable number of employees who have access to make full changes in the SF system. ***No issues noted.***

**Key General IT Control #2:** After each update to tuition table rate information, the SF Accounting Manager haphazardly selects small samples of students and performs a recalculation, to ensure that the ctcLink auto-calculation is functioning correctly.

To confirm this general IT control, we obtained screenshots of the recalculation process that Diana Plum, SF Account Manager, performs. We first reviewed the following amounts shown prior to the recalculation: tuition building fee \$163.76, tuition operating fee \$1,147.05, and tuition S&A fee \$153.97 totaling \$1,464.78. We then reviewed the screen that shows student tuition calculation details like the term, primary program, tuition residency, tuition group, and tuition calc date and time. From there, Diana clicks the calculate tuition and fees button that recalculates tuition from that screen. We noted after the recalculation, those three tuition charges aligned exactly with the original amounts listed in the student account totaling \$1,464.78. We then reviewed a screenshot of the student account details showing the term (Fall 2024), residency (in-state), and credits (13) that we tied to the current tuition schedule to ensure tuition was calculated correctly. ***No issues noted.***

### **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at MAX.

### **J.3.PRГ - Community & Tech College Testing - Spokane**

*Procedure Step:* Charges for Services - Testing

*Prepared By:* JAG, 10/16/2024

*Reviewed By:* RKM, 10/21/2024



# State of Washington

Purpose/Conclusion:

**Purpose:**

To determine whether reported revenues represent actual amounts relating to the period (Occurrence).

To determine whether revenues were reported at properly valued or calculated amounts (Valuation).

**Conclusion:**

We determined that reported revenues represented actual amounts relating to the period (Occurrence) and were properly calculated (Valuation).

**No issues noted.**

Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

For revenues received from the State Treasurer, trace reported amounts to the State Treasurer confirmations available in LGCS.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

**Cut-Off / Revenue Recognition**

Test a sample of underlying transactions to verify the revenue was recorded for the proper period. Note: transactions at the beginning and end of the period would generally be considered at highest risk of being improperly recorded in the current period.

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

**Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

**Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

## State of Washington

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Calculation**

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.

For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.

Review related-party transactions to determine whether revenue transactions were correctly calculated.

### **Realizable Value**

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### **Estimation / Recognition**

Review calculation and support for assumptions of any estimated revenues.

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

Guidance/Criteria:

Record of Work Done:

### **Significant Balances and Assertions:**

Governmental Activities - Education - Higher Education Charges for Services - Occurrence, Valuation

# State of Washington

## Higher Education Special Revenue - Charges for Services - Occurrence, Valuation

Controls are documented in the "Charges for Services - Controls".

We agreed our testing population and college-reported GL data to that which was reported in EIS and in AFRS queries found at: [\[Final Planning Community Colleges Selected for Testing\]](#). **No issues noted.**

Using the TeamStore sampling spreadsheet, we randomly selected 30 students for testing. Our testing selections were made from a report obtained from Tiffany Henderson (Director of Financial Reporting) titled 'SF Accounting Line - Revenue'. We pivoted this report to show the breakdown of total tuition charges by term for each student. See testing at: [\[Charges for Services Testing\]](#).

We requested billing statements and ctclink Campus Solutions (CS) student account information, as well as the FY24 Board-approved tuition rate tables. These were provided by Tiffany Henderson.

### **Substantive Tests Performed to Meet the Occurrence and Valuation assertion:**

See testing here: [\[Charges for Services Testing\]](#)

In order to determine whether reported revenue information occurred, we traced student ID numbers to GL data, billing statements, and CS student account information, noting that information was consistent across these three sources. We also verified that the reported revenue occurred during the correct term (spring, summer, fall, winter) and fiscal year (2024).

In order to determine whether reported revenue information was reported at the correct valuation, we re-calculated the amount billed to students, using the following data from the student profile: residency status, credit division, and credit load. This input data was used to find the tuition rate and fees which should have been assessed per the FY24 Board-approved tuition rate tables. We then adjusted for various waivers, dropped classes, etc.

We determined that reported revenues represented actual amounts relating to the period (occurrence), and were properly calculated (valuation). **No issues noted.**

### **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* Education Expenses - Controls

*Prepared By:* NJH, 10/14/2024

# State of Washington

Reviewed By: RKM, 10/14/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

**Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

**STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-*

# State of Washington

*Level Controls" step as they relate to this particular system.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

## **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

## **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted,*

## State of Washington

*auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

**Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities- Education- Higher Education Expenses - Completeness, Classification

Higher Education Special Revenue- Charges for Expenses - Completeness, Classification

See lead sheet at: [[Lead Sheet](#)]

**STEP 1: Gain an Understanding of Internal Controls**

**Payroll Expenditures:**

On 9/12/24, we met with Melody Matthews (Director of Human Resources Information Systems), Peter Lubetich (Manager of Payroll & Benefits) & Tiffany Henderson (Director of Financial Reporting) to gain an understanding of internal controls for payroll expenditures at CCS. We inquired and confirmed that there were no notable changes to the processes or staff as it relates to the payroll process for CCS.

**Onboarding/New Hires/Employee Set Up (No change from prior year):**

Prior to recruitment, all position requests are entered into the CCSnet PROS (position request online system). The input fields include position title, position control number, position description, expected hours, full-time vs part-time, and classification. These factors drive the rate of pay (such as hourly, exempt, etc.). This system tracks and shows all approval chains related to the position (including budgetary approval). These approvals include the originator, their immediate supervisor, executive approval, budgetary approval, and finally Melody's approval. Any new, full-time permanent positions require a 2nd staffing review after all other approvals have been signed off on. Prior to signing her approval, Melody reviews the Position Request to determine that all information is completed and correct, with no missing fields. She ensures that vacant positions are not being filled twice. After approving, Melody changes the status to 'recruiting', and the system then automatically posts the open position on the College webpage. At this point, a screening committee is responsible for conducting interviews and extending job offers. Once the committee decides to move forward with an applicant, they change the position request status to 'hired', which pushes a notification to Melody's HR team. HR is responsible for ensuring that the new employee completes the new hire application packet. Once the paperwork is complete, it's entered

## State of Washington

into ctcLink, and HR proceeds with employee 'set-up' in the system, including payroll set-up. On the ctcLink Payroll and Compensation screens, HR sets the appropriate job code, status (exempt vs. non-exempt), and salary information (range and step), ensuring that the information entered matches the approved Position Request. ctcLink then automatically calculates the salary from tables, based on these inputs. The Classified salary schedules are maintained by OFM, sent to SBCTC, and then uploaded on behalf of CCS. For professional exempt and faculty schedules, Melody is the individual designated to update these salary lookup tables, based on Board approvals. Budget changes are only allowed on the 1st or the 15th of the month. There are no mid-pay period changes allowed. Every time that an employee change is made (new employee, promotion, reclassification), then HR checks to ensure that ctcLink is correctly calculating the wage for that employee. Spot-checks are also done whenever salary schedules are updated. ctcLink has certain built-in security features to prevent undesirable access to payroll information. The only individuals with system access to update payroll lookup tables are Melody Mathews and Tiffany Henderson. As another example, an individual cannot update their own payroll information, such as giving themselves a promotion or changing their job class. ctcLink also disallows retroactive payments.

### Promotions, COLAs, & Separations:

An Employee Action Notice (EAN) is required for any job location change, supervisor change, stipend, pay increase, or re-allocation. Each EAN goes through the same approval process as Position Requests. A justification also has to be provided with each EAN, showing the original letter for reallocation analysis and a new job description. EAN's contains the chart string/fund information used to correctly classify payroll depending on the employee's assigned exemption status, and is reviewed by budget managers, department managers and HR (**Key Control #1 - Manual - Classification**). Once the EAN and justification are approved, the HR team accordingly adjusts the employee's ctcLink inputs for the Payroll and Compensation screens. Promotions are handled slightly differently - all promotions require a Position Request form for the open position, and the process is then very similar to that of adding a new employee. When an employee separates, an EAN is required, and the letter of resignation or notice of termination must be attached. Separations are not allowed to be backdated. Once an EAN is submitted, HR makes the necessary adjustments in the ctcLink Payroll and Compensation screens. These screens include certain check boxes, such as 'forward to payroll', which pushes out a notification to the payroll team responsible for auditing leave balances. The notification is also forwarded to IT, who removes all ctcLink permissions for the separating employee.

### Processing Payroll:

CCS maintains a 'Payroll' sub folder on their Share Drive, where HR maintains a spreadsheet for new hires and separations, including employee type, start/end dates, etc. This ensures that Peter's team in payroll and benefits is aware of personnel changes where action is needed on their end. Payroll begins processing for each cycle the day prior to the state cut-off date. The payroll team reviews the electronically-submitted time cards, ensuring that all employees have loaded in their time for the correct period, and that it was properly approved (**Key Control #2 - Manual - Completeness**). Leave is tracked manually by the payroll department, and is entered as needed into the system. Once the payroll team has verified that time and leave entries are correct, then they use the 'create pay sheet' ctcLink feature, which pulls in time, leave, and pay rate data for each employee, creating each paycheck. The Department compares job data information to the generated pay processing data. They verify that no employees are missed, and that separated staff are properly excluded, using VLookup formulas. Payroll then follows a Department Task List, Payroll Cycle Timeline, and a Payroll Coordinator Checklist, which requires them to run various queries, perform reconciliations, and follow-up



## State of Washington

on any unusual situations (**Key Control #3 - Manual - Completeness**). Once completed, the system is asked to validate the information, and it is subsequently forwarded to SBCTC. When processed and approved by SBCTC, it is then automatically posted to the GL in ctcLink as a credit to the proper A/P account (Wages Payable), and a debit to the related expense account (Payroll Expense), and another JV is then posted by Peter's team after a review of what checks need to be issued to debit the liability and record a credit to cash paid out.

### **Purchases & A/P:**

On 9/13/23, we met with Heather Pedersen (Account Expensing Supervisor), Tiffany Henderson (Director of Financial Reporting), and Yabing Fisher (Expense Accountant), to gain an understanding of internal controls for general expenditures at CCS.

#### Purchasing/Expense Process:

All new purchase requests are entered into ctcLink through an AP module. Departments create requisitions within ctcLink for the purchase of a service or supply they are requesting. For routine purchases, or those made within pre-determined buying limits (which vary by Department), the purchaser creates a Purchase Order. This includes information such as the supplier number, dollar amount, how the expenses should be charged (budgetary information), signatures (from the originator and the approving supervisor), as well as any comments for the specific purchase. For larger purchases, after gaining budgetary approval from the Budget Department, the request is sent to the purchasing order supervisor, who reviews the Purchase Order request, verifying that all needed information is complete, and that policies and state law are being followed, including review for whether there are any existing contracts affecting the request, if the request can process as a direct buy, or if the process needs to be put on hold until a bid takes place. After Purchase Orders are approved, the Department and originator are able to proceed with the purchase. Once the purchase is complete, the invoice is added to the documentation, and the packet is then sent to the 'AP inbox'. The invoice or receipt is attached as supporting paperwork, and the packet is sent to an 'AP inbox', which captures all submitted payment requests.

#### Purchase Cards (No change from prior year):

Each card has its own limits, which are determined by the requesting supervisor. Heather is responsible for setting up the card with the requested limits. Limit increases, whether temporary or permanent, require a supervisory request be sent to Heather, who will review the request and either authorize or deny the increase. Pre-approval is not required for purchases made within the purchasing limits. Card users are trained on appropriate practices, and then each purchase is reviewed prior to ultimate payment. Staff accountants are responsible for reviewing and auditing purchase card transactions on a daily basis. Once staff marks transactions as 'verified', Heather performs a secondary review of these transactions. Daily, Heather runs a ctcLink cycle which pushes the approved transactions to AP. This creates vouchers, which show up in the twice-weekly pay cycle. When the pay cycle is run, payment is remitted to JP Morgan.

#### Recording Purchases to GL:

On a daily basis, Heather and her team of AP staff sort through the "AP Inbox" to begin manually inputting the relevant purchasing information and the request for payment in the AP module in ctcLink. Once submitted, ctcLink automatically generates a JV that posts the liability and expense entry to the GL. Two times a week, the AP department runs pay cycles, which generate the actual payment (either ACH or physical check). Prior to final batching and processing of the pay cycle, Yabing Fisher (Expense Accountant) reviews and approves all payment vouchers

## State of Washington

and their supporting documentation that was input by the AP staff to ensure that all supporting documentation is complete and is properly approved, that submitted invoice dates are current and reasonable, and that purchases are allocated to the correct fund. For fund classification Yabing noted that she specifically relies on the OFM SAAM Manual to ensure that the fund is classified correctly based on the nature of the purchases (**Key Control #4 - Manual - Classification/Completeness**). Once reviewed, the voucher is submitted as part of the pay cycle, which generates the actual payment (either ACH or physical check) and debits the liability which was previously generated, and credits cash.

### A/P Accruals:

We inquired about the year-end accrual process as it relates to purchase orders or vouchers that might be outstanding after FYE as of June 30th, 2024. At the close of the end of the year, Tiffany will download an export from ctcLink for the month of July showing all of the A/P vouchers that have been submitted at or near the end of the year. She will then route this spreadsheet to the accruals team within the budgeting department, where they will review each voucher separately and make an adjusting JV for any liability or expense that should be recorded or reversed as of the year end date (**Key Control #5 - Manual - Completeness**).

### **Key Controls:**

**Key Control #1 (Manual - Classification):** EAN contains the chart string/fund information used to correctly classify payroll depending on the employee's assigned exemption status and is reviewed by budget managers, department managers and HR.

**Key Control #2 (Manual - Completeness):** Payroll begins processing for each cycle the day prior to the state cut-off date. The payroll team reviews the electronically-submitted time cards, ensuring that all employees have loaded in their time for the correct period, and that it was properly approved.

**Key Control #3 (Manual - Completeness):** The Department compares job data information to the generated pay processing data. They verify that no employees are missed, and that separated staff are properly excluded, using VLookup formulas. Payroll then follows a Department Task List, Payroll Cycle Timeline, and a Payroll Coordinator Checklist, which requires them to run various queries, perform reconciliations, and follow-up on any unusual situations.

**Key Control #4 (Manual - Classification / Completeness):** Yabing Fisher (Expense Accountant) reviews and approves all payment vouchers and their invoices, purchase orders, & receipts that were input by the AP staff to ensure that all supporting documentation (invoices, purchase orders, & receipts) that make up the purchase is complete and is properly approved, that submitted invoice dates are current and reasonable, and that purchases are allocated to the correct fund. For fund classification Yabing noted that she specifically relies on the OFM SAAM Manual to ensure that the fund is classified correctly based on the nature of the purchases.

**Key Control #5 (Manual - Completeness):** Tiffany Henderson, Director of Financial Reporting, will download an export from ctcLink for the month of July showing all of the A/P vouchers that have been submitted at or near the end of the year. She will then route this spreadsheet to the accruals team within the budgeting department, where they will review each voucher separately and make an adjusting JV for any liability or expense that should be recorded or reversed as of the year end date.

### Identified Weaknesses:

**None**

# State of Washington

## **STEP 2: Confirm Key Controls**

**Key Control #1 (Manual - Classification):** EAN contains the chart string/fund information used to correctly classify payroll depending on the employee's assigned exemption status, and is reviewed by budget mangers, department managers and HR.

To confirm this key control, Melody Matthews (Director of Human Resources Information Systems), performed a walkthrough on 9/12/24 of an "EAN *ctcLink ID 101058751*" which showed the the effective date for this EAN in the comments of 7/1/23. We noted that the budget field had the following information: 7170-001-101-083-14200-14201 which we determined contained the the operating unit, the fund, the class, the department and the program numbers. For this particular payroll EAN change we noted the fund to be correctly classified under 001. We then reviewed the chain of sign-offs for this EAN and noted 4 separate sign off's, the last one taking place after fiscal year end on 8/16/24 by Kaitlyn G. Kepner, HRO. No issues noted.

**Key Control #2 (Manual - Completeness / Classification):** Payroll begins processing for each cycle the day prior to the state cut-off date. The payroll team reviews the electronically-submitted time cards, ensuring that all employees have loaded in their time for the correct period, and that it was properly approved.

To confirm this key control we obtained and inspected copies of the following reports provided by Tiffany Henderson, Dir. of Financial Reporting, on 10/14/24 on behalf of Peter Lubetich, Manager of Payroll & Benefits:

06B Confirm Timeline

06B Payroll Task List

06B CTC\_TL\_PAY\_TIME\_BY\_PERIOD.xlsx

We first analyzed the *06B CTC\_TL\_PAY\_TIME\_BY\_PERIOD* spreadsheet showing all of the submitted time sheets and hours for the payroll period of 6/16/24 to 6/30/24. To verify no time sheets were submitted after the cut-off date identified in the *06B Timeline* of 7/1/24, we created a pivot table to analyze the payroll data based on dates provided in the spreadsheet, and noted no dates outside of the acceptable pay range (6/16 - 6/30). We then reviewed the corresponding pay period task list and identified the following steps that were signed off on by "All" on 7/1/24 and 7/2/24 marking them as completed:

*"The morning that time sheets are due to be approved by the supervisor, run the REQUEST TIME ADMIN every half hour to push the submitted hours to the supervisor for approval."*

*"Run the Exception Query periodically to stay on top of the exception errors that have been reported. "*

After reviewing these processes regarding the 06B payroll cycle, we can confirm that the timecards were submitted in the correct period, and that it was properly approved by appropriate staff. ***No issues noted.***

**Key Control #3 (Manual - Completeness):** The Department compares job data information to the generated pay processing data. They verify

## State of Washington

that no employees are missed, and that separated staff are properly excluded, using VLookup formulas. Payroll then follows a Department Task List, Payroll Cycle Timeline, and a Payroll Coordinator Checklist, which requires them to run various queries, perform reconciliations, and follow-up on any unusual situations.

To confirm this key control, Peter Lubetich, Manager of Payroll & Benefits, performed a walkthrough of the payroll process on 9/12/24 for the payroll period of *Payroll Cycle 06A* (the first payroll cycle for June, of FY24). He showed us the payroll timeline spreadsheet for this pay cycle, and we were able to identify that on Friday, 6/14/24, supervisors and managers from each department must submit their time sheets for approval by EOD. ***No issues noted.***

Additionally, Peter showed us the completed Coordinator Processing Checklist, where we were able to identify three steps that were marked as checked off (indicated by an "X") for the following payroll processes for this pay cycle:

Run Pre-Sheet Audit Report (PAY034)

Create Paysheets (PSPPYBLD)

Review Pay Calendar

***No issues noted.***

We also reviewed the *Payroll Department Task List for the Pay Cycle 06A*, and identified a pre-payroll task of "Review leave types taken vs pay groups, etc." by running the "OHC\_AB\_LEAVE\_TYPE\_REASON" ctcLink query. This checklist step was marked completed on 6/18/24 with initial "PLG" which we confirmed was Peter. ***No issues noted.***

**Key Control #4 (Manual - Classification / Completeness):** Yabing Fisher (Expense Accountant) reviews and approves all payment vouchers and their supporting documentation that was input by the AP staff to ensure that all supporting documentation is complete and is properly approved, that submitted invoice dates are current and reasonable, and that purchases are allocated to the correct fund. For fund classification Yabing noted that she specifically relies on the OFM SAAM Manual to ensure that the fund is classified correctly based on the nature of the purchases.

To confirm this key control, Yabing Fisher performed a walkthrough of her review process for *A/P Voucher 00052387* from an invoice on 8/13/24. She showed us the Voucher attachments (supporting documentation) that was uploaded by the A/P team on 9/13/24 which included the Purchase Order from the purchasing department for the supplier *Community PlayThings*, the actual invoice from the supplier, and the purchase approval message thread. Yabing's review included scanning these supporting documents for all necessary information in the ctcLink chartstrings to verify that they were accurate and complete. Additionally, she made sure that the Fund Code and GL Account (Fund 145 and Acct. 5030070) were reasonable based on the purchase by comparing it with the corresponding SAAM manual. We were able to verify that this voucher was thoroughly reviewed prior to being approved by Yabing and being posted to the GL. ***No issues noted.***

**Key Control #5 (Manual - Completeness):** Tiffany Henderson, Director of Financial Reporting, will download an export from ctcLink for the

## State of Washington

month of July showing all of the A/P vouchers that have been submitted at or near the end of the year. She will then route this spreadsheet to the accruals team within the budgeting department, where they will review each voucher separately and make an adjusting JV for any liability or expense that should be recorded or reversed as of the year end date.

To confirm this key control, we obtained and inspected the following documents pertaining to the AP accrual process received by Tiffany Henderson, Dir. of Financial Reporting on 9/19/24:

Accrual List.png

AP Invoices for FY24 needing accruals email thread

Voucher for Adjusting JV

AP Invoice

We first identified that there were services billed to Spokane Falls CC in the amount of \$10,905.44 from the vendor "GoJoePatrol" with an invoice date of 6/30/24. Per the Accrual List report, we identified Journal ID AP00490030 for the posted voucher of \$10,905.44 to record the liability with an invoice date of 6/30/24 and an accounting date of 7/22/24. We then reviewed the email thread sent from Tiffany Henderson to multiple recipients of the budget and fiscal team at CCS with the subject "AP Invoices for FY24 needing accruals" whereby we confirmed that she explained the process the budget team must follow to properly record and post adjusting JV's by creating pivot tables and analyzing invoice dates with 6/30/24 or earlier and accounting dates of 7/1/24 or later. We then reviewed the adjusting JV for this transaction with Journal ID "0000488443" dated for 6/30/24 and posted to period 13 (adjusting period after year end) to post the accrual. We confirmed that the accrual adjustment process is currently in place for FY24. *No issues noted.*

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **J.3.PR.G - Community & Tech College Testing - Spokane**

# State of Washington

*Procedure Step:* Education Expenses - Testing  
*Prepared By:* NJH, 10/15/2024  
*Reviewed By:* RKM, 10/22/2024

## Purpose/Conclusion:

### **Purpose:**

To determine whether reported payable expenditures represent transactions relating to the proper period and to determine whether all payroll expenditures were recorded throughout the fiscal year (Completeness).

To determine whether reported expenses/expenditures were properly allocated in the correct AFRS roll-up funds (Classification).

### **Conclusion:**

We determined that the reported payable expenditures represent transactions relating to the proper period and that all payroll expenditures were recorded throughout the fiscal year (Completeness).

We determined that the reported expenses/expenditures were properly allocated in the correct AFRS roll-up funds (Classification).

## Testing Strategy:

The following is a list of **considerations** for testing the completeness assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Detail Roll-Up**

Compare totals from general ledger to accounts payable, payroll or other subsidiary software modules.

Review the government's reconciliation of general ledger to subsidiary systems.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

### **Cut off / Improper Expense Recognition**

Scan expenditures recorded 1-3 months before and/or after fiscal year end (expenditures not charged to the current period). Based on the scan, test selected or sampled expenditures to determine if the expense should have been reported in the current period.

Inquire with AP clerks regarding invoices held, but not entered as of year-end (ie: due to pending litigation or disputes).

# State of Washington

## **Unrecorded Expenses**

If the entity reconciles recorded revenues and expenses to bank activity, then reviewing monthly reconciliations and evaluating or testing reconciling items.

## **Accounts Payable**

If entity uses a warrant clearing account for vendor payments, review the entity's year-end reconciliation of recorded vendor payments with disbursements from the clearing account.

Review edit check reports from the AP system that might indicate missing payments.

## **Payroll**

If entity uses a payroll clearing account, review the entity's year-end reconciliation of recorded payroll with disbursements from the payroll clearing account.

Perform an expected payroll test by taking the prior audited payroll amount and adjusting it for expected changes.

*The analysis should consider changes in employees, COLA increases, salary scale increases if automatic, changes wages or benefits due to changes in policy or union negotiations changes, etc. Sources for these expectations should be obtained apart from the payroll records that are being tested. Since the auditor would not expect to be able to precisely predict payroll, the auditor should document a reasonable range within which actual payroll is expected to vary from the auditor's prediction.*

If the board directly approves salaries for a significant amount of employees, verify whether the actual salaries for these employees is within an expected reasonable range of the approved salary.

For small entities, compare payroll by employee to known employees per observation, organization charts or a phone list.

Review edit check reports from the payroll system that might indicate missing payments.

## **Unrecorded Liabilities**

Evaluate liabilities directly related to expenses for completeness. See the completeness steps for current and non-current liabilities for testing considerations.

*For example, if the entity reports a self-insurance liability, the auditor might evaluate whether the change in the liability (and related expense) was determined and recorded. If no liability was reported, then the auditor might determine whether such a liability (and associated expense) should have been reported.*

**OPEB** - auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

# State of Washington

**Pollution Remediation** - auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

## **Removing Expenses from Accounting Records**

Search for manual journal entries that credit (decrease) expenditures. Consider testing selected transactions.

Identify transactions that void, cancel, or manually adjust transactions in subsidiary AP or payroll systems. Auditors may conclude that the total amount of such transactions are trivial or otherwise reasonably small. Or auditors may sample or select transactions for testing.

*Also see considerations under the "Not recording expenses" section.*

## **Interfund Expenses**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

The following is a list of **considerations** for testing the classification assertion for expenses/expenditures. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Sample transactions for correct classification. *Use the "Sampling for FS Substantive Testing" spreadsheet available in the Store to calculate sample size and make any projection of likely misstatement to the population.*

If planning has identified a limited population that is high risk (ex: certain transaction types and/or line items within an opinion unit), scan these populations and test selected transactions.

## **Journal Vouchers**

Search for manual journal entries that reclassify expenses/expenditures from one opinion unit to another without recording a balance sheet transaction, other than a direct charge to fund balance (debit and credit to expenditure and fund balance for each opinion unit, respectively). Test selected journal entries based on risk.

Search for manual journal entries that reclassify expenses/expenditures from one line item to another. Test selected journal entries based on risk.

## **Vendor Payments**

Review the top vendors paid by opinion unit or line item (preferably as a multi-year trend) and evaluate whether the vendor meets expectations in relation to the activities of the fund. Test transactions for each unexpected vendor based on risk.

Test selected or sampled transactions for correct classification.

*NOTE: this test may be combined with expenditure tests for other attributes. For example, expenditure testing for accountability or single*



# State of Washington

*audit purposes may also be used for classification testing.*

## **Payroll**

Scan totals charged to each opinion unit by employee (preferably as a multi-year trend) and evaluate whether the allocation of employee's time to that opinion unit meets expectations based on job titles, organization charts, observation or the phone list. Follow up on unexpected allocations by review of timesheets or employee interviews.

Perform an expected payroll test by opinion unit.

Test a sample of pay periods for salaried and hourly employees to ensure that expenditures are being classified to the correct opinion unit. This test should verify both the correct allocation of direct charges and that leave and benefit costs are allocated in the same proportion as direct charges.

## **Cost Allocation Plans / Internal Service Fund Allocations**

Review cost allocation plans or internal service fund charges to confirm that the classification of joint costs to different opinion units is supported. *See example testing strategies for these areas located in the Accountability cabinet .*

Guidance/Criteria:

Record of Work Done:

## **Significant Balances and Assertions:**

Governmental Activities- Education- Higher Education Expenses - Completeness, Classification  
Higher Education Special Revenue- Charges for Expenses - Completeness, Classification

Controls are documented at [[Education Expenses - Controls](#)].

## **Substantive tests performed to meet the Completeness assertion:**

### Accounts Payable

See testing documented at [[CONFIDENTIAL - Education Expenses Testing](#)].

To test the completeness assertion for education expenses (accounts payable), we used the FS sampling spreadsheet set at low assurance to test 30 sampled AP voucher transactions for Q1 in FY25 by running the "QFS\_AP\_VCHR\_ACCTG\_LINE" query in ctcLink. We confirmed population completeness under the "Population Completeness" tab, with no issues noted. We selected a sample containing AP vouchers for accounts 5030010 to 5120030 which represent the majority of Sub object E expenses "Goods & Other Services", and filtered by those accounts within the relevant Higher Education Special Revenue Funds. For each AP sample selected, we analyzed the recorded accounting date as shown in ctcLink compared to the date on the supporting documentation/invoice for each purchase. We also analyzed the description

## State of Washington

and nature of what item/service was purchased to determine if the expense should have been accrued and recorded as an expense during FY24. We obtained a list of all AP Voucher accruals after FYE obtained by Tiffany Henderson, Dir. of Financial Reporting, and cross references these vouchers with our selected sample to determine if any were already reversed and adjusted for during year-end close process.

We identified a total misstatement which is below the floor. ***No issues noted.***

### Payroll

See testing documented at [\[CONFIDENTIAL - Education Expenses Testing\]](#).

To test the completeness assertion for payroll expenses, we used the FS sampling spreadsheet set at low assurance to test 29 sampled payroll employees paid throughout the fiscal year by obtaining the Gross-Net Payroll Spreadsheet from Peter Lubetich (Manager of Payroll & Benefits) showing all payroll activity throughout the year. We confirmed population completeness under the "Population Completeness" tab with no issues noted. For each employee selected, we evaluated the total number of paychecks received throughout the year and compared this with the amount they should have received based on their start / end employment date as provided by HR. Additionally, we reviewed all time sheets and paystubs to ensure that all recorded hours and amounts were properly recorded for the selected pay period.

We determined that payroll expenses were complete throughout the year, and noted no variances. ***No issues noted.***

### **Substantive tests performed to meet the Classification assertion:**

#### Accounts Payable

See testing documented at [\[CONFIDENTIAL - Education Expenses Testing\]](#).

To test the classification assertion for education expenses (accounts payable), we used the FS sampling spreadsheet set at low assurance to test 30 sampled AP voucher transactions for FY24 by running the "QFS\_AP\_VCHR\_ACCTG\_LINE" query in ctcLink. We confirmed population completeness under the "Population Completeness" tab, with no issues noted that would impact our testing. We selected a sample containing AP vouchers for accounts 5030010 to 5120030 which represent the majority of Sub object E expenses "Goods & Other Services", and filtered by those accounts within the relevant Higher Education Special Revenue Funds. We then analyzed invoices, receipts, and purchase orders for each AP Voucher (as applicable) selected for testing to determine if the AP expenditure represented education-related expenses and was classified correctly based on the amount, the vendor, and the nature of the expense.

We determined AP expenditures rolled up to the Higher Education Special Revenue Fund appropriately represent education-type expenses. ***No issues noted.***

### Payroll

See testing documented at [\[CONFIDENTIAL - Education Expenses Testing\]](#).

## State of Washington

To test the classification assertion for payroll expenses, we used the FS sampling spreadsheet set at low assurance to test 29 sampled payroll employees paid throughout the fiscal year by obtaining the Gross-Net Payroll Spreadsheet from Peter Lubetich (Manager of Payroll & Benefits) showing all payroll activity throughout the year. We confirmed population completeness under the "Population Completeness" tab with no issues noted. For each employee selected, we evaluated if the amount of pay received corresponded with education-related services, employment, or temporary contracts as it pertains to payroll expenditures by reviewing supporting HR documentation and knowledge of the college operations regarding payroll.

We determined payroll expenditures rolled up to the Higher Education Special Revenue Fund appropriately represent education-type expenses. ***No issues noted.***

### J.3.PRG - Community & Tech College Testing - Spokane

*Procedure Step:* Federal Grants in-Aid - Controls

*Prepared By:* JAG, 10/7/2024

*Reviewed By:* RKM, 10/8/2024

Purpose/Conclusion.:

**Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

**Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy.:

The following procedures are **required** for all relevant systems:

# State of Washington

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

## **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled*

## State of Washington

*down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

### **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*

## State of Washington

*D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Education - Higher Education Operating Grants and Contributions - Occurrence  
Higher Education Special Revenue - Federal Grants-In-Aid - Occurrence

See lead sheet here: [[Lead Sheet](#)]

# State of Washington

## **STEP 1: Gain an Understanding of Internal Controls**

We met with the following people on 9/16/24 to update our understanding over federal grants-in-aid:

Tiffany Henderson, Director of Financial Reporting  
Brandy Browning, Director of Accounting and Budget  
Diana Biddison, Budget Analyst 3 (Non-Financial Aid Grants)

There are several types of federal grants received at Community Colleges of Spokane (CCS) which require separate processes. We have categorized these into two basic grant types: Financial Aid Related (DOE), and Non-Financial Aid Related (DOA, DOL, HHS, etc.)

### Financial Aid Grants:

The financial aid related grants are through the Department of Education (DOE) including, Pell Grants, Federal Supplemental Educational Opportunity Grant (SEOG), and Federal Work Study Program (FWS).

### Expenses:

To be eligible for federal awards, students fill out the FAFSA and DOE determines eligibility based on different criteria for each grant. Review of eligibility and awarding is determined on campus in the Financial Aid Office (FAO). Once the amount of federal aid has been determined, the FAO sends students award letters and lets them know the dollar amounts of their awards. In the disbursement phase of the process, federal regulations allow them to disburse funds up to 10 days in advance, but CCS does not disburse funds in advance and students don't have access to the funding until the first day of the quarter. CCS has an established disbursement process where they work together with the student finance office to separate the duties of award and disbursement. CCS staff in the FAO, normally the Associate Director or a Disbursement Specialist, runs a predefined disbursement process which is a query that checks for enrollment, if any factors have changed, and continued eligibility within the system. The FAO then sends the Manager of Student Accounting, Diana Plum, a file containing a list of all student accounts and the amounts that are to be disbursed. Diana uploads it as a batch to Bank Mobile to apply the awarded amounts to those student's accounts. The file from the FAO contains item types that have a string of coding to the chart of accounts so they post to the correct grant.

DOE grants also allow for a certain percentage of indirect costs to be included for reimbursement. CCS has an approved indirect cost rate plan, but if there is a determined rate inside the grant agreement itself, then the rate in the agreement will be used. The FAO calculates the expenditure amount with the correct indirect cost rate with the Manager of Student Accounting's assistance.

### Reimbursement:

Once the awards to student accounts have been posted, the Manager of Student Accounting runs queries out of the accounting software to determine how much has been applied to each type of grant. The Manager of Student Accounting pulls the reports for the entire grant award period to date (which is the start of the FY) from the Student Management subledger. These reports contain lists of student accounts in which the funds were applied. The Manager of Student Accounting performs a reconciliation, taking the total revenue already received and subtracting it from total expenditures to obtain the total draw amount and to ensure all applicable expenditures are included in the draw request and are for the

## State of Washington

correct period **(Key Control 1)**.

In order to avoid overdrawing and having to return funds, the Manager of Student Accounting will draw slightly less (depending on the grant, average of \$50k) than the actual calculation. The amount is determined based on experience with the grants and professional judgement. Draw downs from the online G5 system are based on actual expenditures. G5 is the DOE's grants management system designed to track grant awards and issue reimbursement. Draw downs are submitted approximately 3 days prior to the start of each school quarter and then another around two weeks after the quarter starts. Then approximately once a month for the rest of the term. This allows for students to have had a chance to finalize their schedules with any classes added or dropped. Because tuition expenses are constantly a moving target, at the end of the FY the Manager of Student Accounting does a true-up reconciliation (with Financial Aid and G5) by running detailed expenditure reports from the CCS accounting system and balancing to the total expenditures tracked in G5. The Manager of Student Accounting ensures that only the transactions related to the applicable grant year are included by running expenditure reports by student term (winter, spring, summer, fall).

Tiffany stated that they do occasionally need to make corrections for recording expenses or revenues in the wrong period. This is especially true for activity on the last day of the month or at the end of the fiscal year. Errors are caught during reconciliations and in order to make the correction, fiscal analysts create accrual entries to move the revenues and expenses to the correct fiscal period.

### Revenue Recognition:

The Manager of Student Accounting sets up an AR and revenue when funds are requested. Once the draw from the G5 system has been approved, funds are electronically transferred into the College's bank account. A verification email is received from the grantor/agency documenting the EFT transmission which is used to apply funds to the appropriate invoices (A/R). The FA2 who performs the daily cash reconciliations, Laurice May, clears the receivable to recognize the revenue.

### Non-Financial Aid Grants:

Non-financial aid related grants are through the Department of Labor (DOL), Health and Human Services (HHS), etc.

### Expenses:

At each of the colleges, program managers are responsible for approving purchases (generally using P-Cards) for allowable activities as well as reviewing and approving the payroll/travel in which employees charge time to various grants. Billings are reviewed again at the District Office for reasonableness and are then approved for payment through the normal AP process. All receipts and backup documentation are attached in the billing system to support transactions. Once the expenditures have been paid, the Fiscal and Budget Analysts are able to review the supporting documents for reasonableness (based on the specific grant) and to ensure the expense are properly valued and recorded in the appropriate period prior to requesting reimbursement. As mentioned above, the college has an approved indirect cost rate plan and costs for the period are calculated and entered by Diana prior to requesting reimbursement using the rate from this plan, or the rate from the grant agreement if specified to do so. Credits are recorded as reducing the correlating expenditure and are picked up in the expenditure detail report. Additionally, when billings are recorded at fiscal year end, they are accrued back into the appropriate period so that when the revenue is recognized, it is being



## State of Washington

accrued back and applied to the correlating expenditure.

### Reimbursement:

For state board grants, OBIS (Online Budget & Invoicing System) is billed first and then the billing is done in the grant module to calculate the revenue for reimbursement; non state board grants require the creation and submission of a pre-approved reimbursement request template. At the end of the month (or quarterly depending on the grant agreement) the Fiscal or Budget Analyst runs expenditure reports from the GL and balance these reports to the Colleges billing module to ensure that all expenditures are included and are for the correct period. The Fiscal and Budget Analyst use the GL actual expenditures report to prepare the reimbursements (**Key Control 2**). For grants requiring a template, the reimbursement request is given to the Manager of Student Accounting to review and submit. The Fiscal and Budget Analyst review expenditure detail and monitor grant budgets to ensure that the expenditures are for the correct fiscal year. Diana stated that the college uses the fixed price billing method to bill all their grants in ctclink so that no CAPC journals are produced. They do have grants that are cost reimbursable and grants that are fixed price grants. For cost reimbursable grants, the calculation of revenue for reimbursement is determined by the amount of expenditures charged to the grant for the month. For fixed price grants, the calculation of revenue for reimbursement is determined by the grant contract, which either specifies how much to bill each month or specifies how to determine how much to bill each month/quarter. CCS bills both types of grants under the fixed price billing method in ctclink. All grants are recorded in the GL and grant bills are picked up by running a GL report. The GL grant report is balanced and expenditures are reviewed by the Fiscal and Budget Analyst to ensure all bills were reconciled for the period.

### Revenue Recognition:

As all grants are processed under the fixed price billing method, CCS avoids creating excess revenue entries through unbilled receivable (CAPC) journals. OBIS is manually billed where a JE is created to debit AR control and credit revenue. Upon EFT of the funds from the granting agency, the receivable amount is reduced by the treasury clerk using the EFT detail to apply to the correct AR invoice.

Note: The information in the accounting system, which is a result of the processes above, is gathered for reporting at the state level.

### Key Controls:

**Key Control #1 (Occurrence - Financial Aid):** The Manager of Student Accounting performs a reconciliation, taking the total revenue already received and subtracting it from total expenditures to obtain the total draw amount and to ensure all applicable expenditures are included in the draw request and are for the correct period.

**Key Control #2 (Occurrence - Non-Financial Aid):** The Fiscal and Budget Analyst, use expenditure reports for the grant period to date and balances these reports to the College's billing module to ensure that all expenditures are included and are for the correct period. Once determined, the correct entry is made - (DR) receivable / (CR) revenue.

### Identified Weaknesses:

**None.**

# State of Washington

## **STEP 2: Confirm Key Controls**

**Key Control #1 (Occurrence - Financial Aid):** The Manager of Student Accounting performs a reconciliation, taking the total revenue already received and subtracting it from total expenditures to obtain the total draw amount and to ensure all applicable expenditures are included in the draw request and are for the correct period.

We obtained two reconciliation spreadsheets "Workpapers - SP24 3.15 Draw" and "23-24 Master Recon - t. March 2024 - SCC Federal" from Tiffany Henderson, Director of Financial Reporting. The spreadsheet was prepared by Brooke Sackman, Manager of Student Accounting. The spreadsheet shows disbursements for the period 3/1/24-3/30/24 for CARES, SEOG, DL and Pell. The reconciliation includes tabs with detailed expenditure data, including payment dates, from ctLink to support the amounts reported as disbursed for the period. The reconciliation also includes a calculation of the amount to draw, which was underdrawn to keep a buffer. The reconciliation notes a draw of the following amounts:

WA171 and WA172 CARES - \$0  
WA171 SEOG - \$13,080  
WA172 SEOG - \$7,335  
WA171 DL - \$154,652  
WA172 DL - \$79,145  
WA171 Pell - \$295,312.95  
WA172 Pell - \$1,575,794.94  
Total \$2,125,319.89

We viewed a screenshot showing the G5 draw confirmation that tied to amounts from the recon, with a deposit date of April 30, 2024. We traced these to the April Bank of America bank statement, showing deposits made on 4/30/24 in the total amount of \$2,125,319.89. We also obtained the related invoices (MSC-0000028015 & MSC-0000027986) and the portal funds request email sent from Brooke Sackman to WSAC dated 4/29/24. We noted that the draws on the spreadsheet, invoice, bank statement, and the portal funds request email tied without exception. ***No issues noted.***

**Key Control #2 (Occurrence - Non-Financial Aid):** The Fiscal and Budget Analyst, use expenditure reports for the grant period to date and balances these reports to the College's billing module to ensure that all expenditures are included and are for the correct period.

We obtained the June 2024 Head Start draw back up documentation "SMARTLK #710" dated 7/23/24. The total for this draw per the billing module was \$883,805.31. We saw email communication noting the draw was prepared by Brandy Browning, and approved and submitted by Diana Biddison. The packet included a screen shot from the Department of Health and Human Services' Payment Management System and two invoices CA-0000019493 and that tied to the same amount. We viewed detailed expenditure activity that tied to the draw amount. ***No issues***

# State of Washington

*noted.*

## **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **J.3.PR.G - Community & Tech College Testing - Spokane**

*Procedure Step:* Federal Grants in-Aid - Testing

*Prepared By:* JAG, 10/16/2024

*Reviewed By:* RKM, 10/21/2024

Purpose/Conclusion.:

### **Purpose:**

To determine whether reported revenues represent actual amounts relating to the period (Occurrence).

### **Conclusion:**

We determined that reported revenues represent actual amounts relating to the period (Occurrence). **No issues noted.**

Testing Strategy.:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

# State of Washington

For revenues received from the State Treasurer, trace reported amounts to the State Treasurer confirmations available in LGCS.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

## **Cut-Off / Revenue Recognition**

Test a sample of underlying transactions to verify the revenue was recorded for the proper period. Note: transactions at the beginning and end of the period would generally be considered at highest risk of being improperly recorded in the current period.

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

## **Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

## **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

Guidance/Criteria:

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

## **BARS [3.6.9](#) Revenue Accruals in Governmental Funds**

# State of Washington

Record of Work Done:

## **Significant Balances and Assertions:**

Governmental Activities - Education - Higher Education Operating Grants and Contributions - Occurrence  
Higher Education Special Revenue - Federal Grants-In-Aid - Occurrence

Controls are documented in the "Federal Grants-In-Aid - Controls" step.

## **Substantive tests performed to meet the Occurrence assertion:**

Reconciliation: [Federal Grants In Aid Testing]

We obtained AFRS data for CCS Federal Grants in Aid and Higher Education Operating Grants and Contributions from the ACFR database, as shown here: [Final Planning Community Colleges Selected for Testing]. We analyzed the data and determined 100% of the federal grants in aid balance and 66% of the higher education operating grants and contributions balance were comprised of revenue from the Department of Education and the Department of Health and Human Services (funds 145 and 846 for sources 384 and 393). We determined to focus our testing on these two sources as they provide sufficient coverage of the balances.

We utilized the ctcLink crosswalk to determine that these AFRS revenue source codes translate to ctcLink accounts 4022280 and 4022290. We obtained FY24 Grant revenue for funds 145 and 846 from Tiffany Henderson, Director of Financial Reporting. We determined amounts tied without exception between AFRS/ctcLink.

Sample Selection and Testing: DOE [Federal Grants In Aid Testing] and HHS [Federal Grants In Aid Testing]

We utilized the sampling spreadsheet for populations of 365 or less to determine sample sizes (13 for DOE and 11 for HHS). We noted no individually significant items. To test that reported revenue occurred during the fiscal period and was supported by adequate documentation, we received the following for each sample from Tiffany Henderson, Director of Financial Reporting:

- GL data showing expenditures and the reconciliation performed to determine the amount of funds to draw

- Invoices showing the amount requested for reimbursement

- Screen shots from the G5 system showing confirmation of the payment request

- Email confirmations from G5 showing the payment request has been processed and will be deposited in the college's bank account

- For HHS Head Start samples, we received invoices, SMARTLK billings showing a breakdown of the amount to draw along with expenditure reports that tied to the draw amount, and screen shots from the HHS Payment Management System showing the ACH payment

We traced sampled revenues from the GL to GL data, supporting billings or subsequent receipts to verify recorded revenue occurred during the period and was adequately supported. ***No issues noted.***

# State of Washington

## J.4.PR.G - Community & Tech College Testing - Bellevue

*Procedure Step:* Summary & Conclusion

*Prepared By:* JLE, 10/17/2024

*Reviewed By:* RKM, 10/28/2024

Purpose/Conclusion:

### **Purpose**

To evaluate risk assessments and the sufficiency and appropriateness of evidence obtained based on results of substantive work.

### **Conclusion**

We determined that **no modifications** were necessary to inherent risk, control risk or the risk of material misstatement as assessed in planning.

We also determined that evidence obtained was sufficient and appropriate in response to the risk of material misstatement.

Testing Strategy:

Auditors are **required** to evaluate conclusions for substantive testing as follows:

*Auditors may wish to use the optional Lead Sheet available in the Store to summarize testing related to each balance and assertion.*

**1.** Determine whether the results of substantive testing indicate a need to modify the inherent risk assessment (IR), control risk assessment (CR), risk of material misstatement (RMM) or other aspects of planning (such as material balances or assertions). If so, document changes and consider the need for additional testing.

*If the results of substantive testing indicate a need to change control risk, auditors should also update the **Permanent File** by either correcting the documentation or by adding an update section describing changes to the top of the record of work done. For all changes to IR, CR, or RMM the **Material Balances** spreadsheet should be updated.*

*More significant changes to other aspects of planning (such as material balances or assertions) should be referenced in this step and documented in detail in the **Changes to FS Audit Plan** step.*

**2.** Evaluate whether the quality and quantity of evidence obtained is sufficient and appropriate in response to the risk of material

# State of Washington

misstatement. In making this determination, auditors should evaluate:

## Information to be used as audit evidence:

- Does evidence relate to the population, period of time and risk (assertion and “what could go wrong” from the Material Balance Spreadsheet)? If there are any gaps or uncertainties in the logical connection between the evidence and conclusions, is there a documented consideration and explanation?
- Are the sources of information sufficiently reliable and appropriate for the risk (whether internal to the government, external, or auditor developed)? If key information is not from a sufficiently reliable source (for example, inquiry), then is it corroborated by information that is?
- Are there any concerns about accuracy, completeness, authenticity, or bias in information? If so, did the auditor perform sufficient procedures to confirm reliability of that information?
- Is information precise enough to catch if misstatements exceeded the tolerable level?
- Is information detailed enough to conclude on whether or not there were misstatements?
- Was there any information that appeared contradictory or inconsistent? If so, was there a documented response to the inconsistencies or doubts about the reliability of evidence?

## Results:

- How much misstatement was identified by testing, and the likelihood and magnitude of further potential misstatement?
- How did misstatements occur and how often might they occur again in the population?
- Were misstatements caused by control deficiencies or circumvention of controls?
  - If control deficiencies, is there a need to re-evaluate our understanding of controls in the [Permanent File](#) folder or assessment of control risk?
  - If circumvention, the [Management Override of Controls](#) step should address or reference this area. Auditors should also consider whether a fraud risk has been identified.
- Did tests identify a different level or type of risk than the planned audit response was designed to address?
- If likely misstatements are identified, are further procedures necessary to improve the precision of our estimate?

*To support the overall evaluation of audit risk and provide a basis for concluding on the overall sufficiency and appropriateness of evidence in the [FS Summary & Report](#) step, auditors should conclude in each area whether the auditor continues to believe that the tests performed and quality and quantity of evidence obtained are commensurate with RMM for all relevant risks (the “what could go wrong”, in the [Material Balances](#) spreadsheet).*

If the auditor determines that evidence is not sufficient or appropriate, additional substantive testing should be done. If sufficient, appropriate evidence is not available for audit, the AIC should discuss the effect on our audit report with the AAM and AM.

# State of Washington

Guidance/Criteria.:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6310](#) – Determining the Nature, Timing and Extent of Substantive Testing**

**SAO Audit Policy [3210](#) – Audit Evidence**

**[Investments](#) area guide**

Record of Work Done.:

Based on test results, we re-evaluated risk assessments, procedures, evidence obtained and conclusions as follows:

### **(1) Do the results of substantive tests indicate a need to modify our risk assessment (IR, CR and RMM)?**

The results of substantive tests do not indicate a need to modify our risk assessment.

### **(2) Was the quality and quantity of evidence obtained sufficient and appropriate?**

The quality and quantity of evidence obtained was sufficient and appropriate.

## **J.4.PRG - Community & Tech College Testing - Bellevue**

*Procedure Step:* Cash and Cash Equivalents - Controls

*Prepared By:* SRC, 10/9/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion.:

### **Purpose:**

To gain an understanding of internal controls over cash and investment reconciliations and assess control risk in order to help plan the nature, timing and extent of substantive testing.



# State of Washington

## **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

## **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

**Expected key control for existence and completeness:** Bank reconciliations are performed timely on at least a monthly basis to ensure the general ledger agrees to bank and investment account records.

*Documentation should include who performs bank reconciliations, how often they are performed and how reconciliations are aggregated and compared to the general ledger.*

# State of Washington

*Note: we would expect additional key controls if the government has any alternative investments or investments subject to significant interest rate or other risks.*

## Expected compensating controls:

An accounting system module or a standard template is used to document reconciliations.

Segregation of duties in that the person performing bank reconciliations does not have cash handling duties or access to initiate disbursements by wire or check.

Timely, independent review of bank reconciliation documentation, including journal entries for adjustments identified from the bank statements (such as fees, NSF checks, etc).

An up-to-date listing of change fund, petty cash and imprest fund accounts is maintained in accordance with BARS 3.8.8.

Zero-balance bank accounts and clearing funds (see BARS 3.8.6) are reconciled to zero on a monthly basis.

If the government has an investment account (that is, other than the State or County LGIP), documented inquiry with their investment service to verify the methodology for determining fair value of investments and the valuation input hierarchy level for purposes of their fair value (GASB 72) disclosures.

*Some investment accounts provide information about its methodology, assumptions, and data in valuing investments at the asset class level. However, brokers often provide no, or only limited, information about the inputs and assumptions used in developing the fair value. Management should either obtain a document with this information or contact the broker/institution to gain an understanding of the information about methods and inputs used in determining the fair value and where the investment should be disclosed in the hierarchy.*

*Contact the Investment Specialist for any questions on expected controls or documentation over fair value disclosures.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person*

## State of Washington

*performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*Suggested confirmation for expected key controls are to obtain and scan all year-end bank reconciliations and supporting documentation. This is normally done in conjunction with substantive testing. We would expect that bank reconciliations would clearly show check figures that compare the aggregated adjusted bank balance to the general ledger.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

### **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it*

## State of Washington

*would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

# State of Washington

## **Significant Balance(s) and Assertion(s):**

Internal controls in the Community and Technical College System address the following balances:

Higher Education Special Revenue Fund - Cash and Cash Equivalents - Existence

Higher Education Student Services Fund - Cash and Cash Equivalents - Existence

See lead sheet here: [[Lead Sheet](#)]

## **1. Gain an Understanding of Internal Controls**

We met with Jennifer McMillan, Finance Manager, via Teams on September 18, 2024 to discuss Bank and Investment Reconciliations at Bellevue College.

### **Cash & Bank Reconciliation**

There are 2 levels of reconciliations done. The first one is done daily within Peoplesoft with a FA5 downloading the bank statement in excel format into the system. This is matched up with AP and AR transactions and it automatically matches up the transactions. There is a screen within the system that shows unreconciled transactions. The second level is a monthly book to bank focusing on cash and GL balances. Jennifer prepares it using eight different queries and reports which are listed in a standard written procedure the College provides for reconciliations. Once the reconciliation is done, it is sent to Ty Bergstrom, Director, for review and approval (**Key Control #1- Existence**). Normally, this process is performed by a FA5 and reviewed by the Finance Manager, but the FA5 position is currently vacant, so Jennifer is preparing the reconciliation and the director is approving.

### **Investments Reconciliation**

The College currently has 8 investment accounts totaling about \$77 million, which change periodically based on maturities and reinvestments.

Jennifer explained she uses a detailed workbook to track investments. The workbook has a tab for each investment which holds all the fundamental data associated with that investment and tracks all anticipated transactions for the life of the investment. There is also a tab with a full schedule of events expected for each investment, such as anticipated accrued interest. Jennifer uses these figures in conjunction with the bank statement to reconcile monthly to the GL and ensure transactions are occurring as they should. The monthly reconciliation is reviewed by the FA5 or Accounting Manager (**Key Control #2 - Existence**)

### **Petty Cash and Change Funds**

The college currently has six departments which utilize change funds: Library Copier, Printing Services, Student Financial Services (SFS), PAL's Center, and Food Services. Each department has a Custodian who is in charge of daily cash counts. The Accounting Manager puts together a monthly Change Fund Balance Sheet to confirm that the amount of cash on hand matches the GL Balance.

## State of Washington

There was a Petty Cash Fund for Student Financial Services, but it was rarely used. The account was closed as of 7/25/24.

### **Summary of Key Control(s):**

**Key Control 1 (Existence):** Jennifer McMillan, Finance Manager, reconciles the GL to bank statements, noting all reconciling items on the reconciliation spreadsheet, then signs the reconciliation form which the Finance Director subsequently reviews for completeness and accuracy.

**Key Control 2 (Existence):** Jennifer McMillan, Finance Manager, performs monthly reconciliations between the workbooks and GL to ensure interest payments, amortizations, balances, and maturities are as expected.

### **Noted Weaknesses are as follows:**

None noted

## **2. Confirm Understanding**

**Key Control 1 (Existence): Jennifer McMillan, Finance Manager, reconciles the GL to bank statements, noting all reconciling items on the reconciliation spreadsheet, then signs the reconciliation form which the Finance Director subsequently reviews for completeness and accuracy.**

We obtained the July 2024 bank to GL reconciliation. We noted reconciling items and it was prepared by Jennifer McMillan, Finance Manager, on 9/18/2024 and signed as reviewed by Tyrell Bergstrom, Executive Director, on 9/18/2024. **No issues noted.**

**Key Control 2 (Existence): Jennifer McMillan, Finance Manager, performs monthly reconciliations between the workbooks and GL to ensure interest payments, amortizations, balances, and maturities are as expected.**

We obtained the 2024 FYE investment reconciliations performed by Jennifer McMillan, Finance Manager, and reviewed by Ty Bergstrom, Executive Director. We noted it was separated by section as follows: Actuals, Should be, Adjust for Prior Year Interest Rev, Final Difference, and Total Current Year Revenue. The Final Difference came out to \$0. **No issues noted.**

## **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **STEP 5: Final Control Risk Assessment**

# State of Washington

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

## J.4.PR.G - Community & Tech College Testing - Bellevue

*Procedure Step:* Cash and Cash Equivalents - Testing

*Prepared By:* SHW, 10/28/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion:

**Purpose:**

To determine whether reported cash and investments existed as of the end of the period.

**Conclusion:**

We determined reported cash and investments existed at the end of the period. *No issues noted.*

Testing Strategy:

**SAO Policy Requirement: Confirming or Verifying Cash & Investment Balances**

Confirmations can either be blind or a positive confirmation. In a blind confirmation (sweep), the auditor requests information on all accounts the bank holds for the entity (by entity name and/or EIN). In a positive confirmation, the auditor lists accounts (or accounts and balances) per the entity and asks the bank to confirm that the information is correct.

Confirm cash and investment account balances with County Treasurer, bank and/or brokerage. Use the template confirmation form provided in the Store when needed.

Confirmations can be mailed to addresses listed on the Bank Confirmation Address List available on the Auditor Reference Guide. If the bank notifies you of a different address, please contact Team Audit Support to update the list.

Banks may confirm incorrect amounts either due to a simple mistake, use of a wrong confirmation date or incorrectly including or excluding accounts. The first step in resolving differences should be to check information against the entity's bank statements and then call the bank to specifically confirm any difference.

## State of Washington

Confirming investments may involve physical inspection, confirmation with the issuer, confirmation with the custodian, confirmation of unsettled transactions with the broker/dealer, confirmation with the counterparty, and/or reading executed partnership or similar agreements. When confirming investments, ensure investments are held in the entity's name.

*If confirmations are not used*, auditors must at minimum verify balances to the County Treasurer, bank and/or brokerage statements. If this is done, the auditor should consider the risk that the statements were altered and should examine papers for indications of alteration.

The following is a list of **additional considerations** for testing the existence assertion for cash and investments. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### Bank Reconciliations

If the auditor is comparing reconciled (confirmed) bank or county treasurer balances to the GL (rather than confirmed amounts within an expected variance due to reconciling items), the auditor should consider performing some or all of the following tests to verify the accuracy of the reconciliations. Note that testing the reconciliation will provide evidence of both the existence and completeness of cash and investment balances.

Trace (or compare summed) bank balances per statements to reconciliations.

Trace (or compare summed) book balances per reconciliations to the general ledger or financial statements.

*If a cash account is allocable to a particular fund, the balance in the general ledger should be recorded in the same fund.*

Scan the reconciliation for reasonableness. Look for unusual, unexpected or vaguely described reconciling items, lack of support or detail, very large reconciling items, very old reconciling items, and missing or extra elements that would indicate that the reconciliation was being performed incorrectly.

Foot the reconciliation for accuracy.

Trace deposits in transit to the subsequent month's bank statement, considering reasonableness of the in-transit period.

Trace outstanding checks to cash disbursement journal.

Check that any other reconciling items are valid and have been properly accounted for (ex: large debit or credit memos).

Check reconciliation against prior and/or subsequent reconciliations for reasonableness of amounts and items included and to trace reconciling items from the previous and/or subsequent period.

### Other Tests

Inquire whether any checks or deposits were being held at year end for budget, cash flow or other purposes.

Confirm investments purchased but not received as of year-end



## State of Washington

Confirm investments sold but still held as of year-end

Confirm interest due or accrued but not yet received as of year-end

Search for manual journal entries that debit (increase) cash. Consider testing if risk indicators are noted.

Review reconciliations of clearing and transmittal accounts.

See accountability steps for testing strategies related to petty cash and imprest funds, which are not expected to be material to the financial statements.

*Auditors may perform additional procedures to confirm information in the deposit and investment note disclosure in this step or in the Notes to the Financial Statements step. Auditors should contact the Investment Specialist if they note significant interest rate or other risks with the government's deposits or investments.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**Outstanding Checks and Deposits in Transit** – Per TIS section 1100.08 (AICPA Technical Questions and Answers), outstanding checks should be reported as a reduction of cash and the amount of deposits in transit should be reported as cash. A check is considered outstanding from the time that it is out of the payor's control – when mailed or delivered to the payee – until the time it clears the bank. Cash should represent amounts within the control of the reporting entity, that is, the amount of cash in banks plus cash and checks on hand and deposits in transit minus the amount of outstanding checks.

**SAO Audit Policy [6350](#) – External Confirmations**

**[Investments](#) Area Guide**

**[LGIP Fund Summary Reports](#)** - includes a list of local government accounts and balances in the Local Government Investment Pool

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.8.6](#) Use of Payroll and Claims Funds**

# State of Washington

Record of Work Done:

## **Significant Balance(s) and Assertion(s):**

Internal controls in the Community and Technical College System address the following balances:

Higher Education Special Revenue Fund - Cash and Cash Equivalents - Existence

Higher Education Student Services Fund - Cash and Cash Equivalents - Existence

Controls are documented in the "Cash and Cash Equivalents - Controls" step.

## **Substantive tests performed to meet the Existence assertion:**

We obtained ctcLink data using the query QFS\_GL\_SNP\_DETAIL, filtered for cash and investments. We obtained AFRS data from the "Trial Balance-Cash and Investments" DARS report. We determined that the AFRS balances tie to ctcLink without exception. See "Balance Breakdown" tab here: [[Cash and Equivalents Testing](#)]. **No issues noted.**

We obtained the June 30, 2024 month-end reconciliation, bank and investment statements, and petty cash counts from Jennifer McMillan, Finance Manager, to verify existence of cash at 6/30/2024. We also obtained the July 2024 ARP Detail Reports to verify reconciling items and outstanding checks. We traced 100% of deposits in transit to the July 2024 bank statement and tied a sample of outstanding checks to the July 2024 ARP Report. See testing in the "Summary" tab at: [[Cash and Equivalents Testing](#)]. We noted an understatement of \$423,702 between the bank reconciliation and the GL. Since this is below the floor, we not take to the aggregation of misstatements.

For outstanding checks, we obtained the US Bank reconciliation report (ARP) and tested a random sample of 38 outstanding checks and two individually significant items. We noted all checks were either cleared in July 2024 or listed as Outstanding or Canceled on the July 2024 ARP Report. See "OS Checks" tab: [[Cash and Equivalents Testing](#)]. **No issues noted.**

Additionally, we obtained the petty cash reconciliation and tied petty cash to GL 1130 in DARS without exception. See "Petty Cash" tab: [[Cash and Equivalents Testing](#)]. **No issues noted.**

## **J.4.PRG - Community & Tech College Testing - Bellevue**

*Procedure Step:* Depreciable Capital Assets - Controls

# State of Washington

*Prepared By:* JLE, 10/14/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion:

## **Purpose**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

## **Conclusion**

We have gained an understanding of internal controls and assessed control risk at '**MAX**'. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

## **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-*

# State of Washington

*Level Controls" step as they relate to this particular system.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

## **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

## **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted,*

## State of Washington

*auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [2310](#) - Reporting Identified Audit Issues

## SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk

## [Financial Statement Audits](#) Planning Guide

Record of Work Done:

### **Significant Balances and Assertions**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Depreciable Assets (Net of Accumulated Depreciation) - Existence, Valuation

See lead sheet here: [[Lead Sheet](#)]

### **STEP 1: Gain an Understanding of Internal Controls**

We gained an understanding of internal controls over depreciable assets via Teams meeting on 9/10/2024 with the following individuals:

Jennifer McMillan (Fiscal Reporting & Student Financial Services Manager)

Sharon Liang (Fiscal Analyst)

### **Asset Additions**

The majority of the College's asset additions fall into two broad categories: buildings (i.e., construction in progress / repairs) and equipment. For buildings, the College has a 'Capital' team tasked with ensuring that costs are appropriately tracked and monitored. This team works directly with contractors to ensure that projects are developed within budget, and adhere to the contract agreement. On a monthly basis, the Capital team submits invoices to the Accounts Payable (AP) department to record costs associated with the projects.

Equipment additions are normally initiated by decentralized departments across the College. Each department has its own budget and procurement needs, and is responsible for submitting Purchase Orders (PO) or Purchase Card requests to the centralized AP department via ctcLink. The main AP accountant is a longstanding experienced employee of the College, and has received frequent internal trainings; as such, they are well-versed in capital asset identification and reporting requirements. When AP recognizes that a PO or invoice represents a capital asset, they ensure that the expense is coded to appropriate accounts (asset expense accounts begin with '504'), and they additionally fill out the 'Profile ID' field (a 4-digit field for SAAM-based commodity codes, which is used to identify the asset's useful life). By updating the Profile ID field, ctcLink is triggered to notify Sharon of the new depreciable asset addition (in some cases, AP will also notify Sharon directly). Sharon then creates an asset within the Asset Management (AM) sub-module of ctcLink, reviewing to ensure that the correct cost and useful life is recorded based applicable POs and invoices (**Key Control 1 - Existence, Valuation**).

## State of Washington

AP also notifies the Receiving team within the warehouse that they will be receiving an order requiring asset ID tags. After the Receiving team confirms receipt of the asset and assigns a tag number, Sharon updates the asset ID field within AM, and also adjusts asset cost for any ancillary costs which weren't already captured (shipping, tax, etc.). On a quarterly basis, Sharon performs a query against expense accounts (primarily focusing on accounts beginning with '503'), reviewing for invoices exceeding the \$5k capitalization threshold, to ensure that there were no expenses representing capital assets which may have been missed by the AP department.

### Asset Inventory and Disposals

The College performs an annual inventory count toward year-end on a rotating basis, tracking half of their recorded inventory in one year, and the remaining half in the subsequent year. The majority of assets which require disposal are identified through the inventory process. The College also identifies disposals via direct notification from various decentralized departments throughout the year. When an asset is identified for disposal, Sharon is tasked with removing the asset from AM, and ensuring that this change was also captured in the general ledger. The vast majority of assets requiring disposal have reached the end of their useful life, and are fully depreciated. Sharon also ensures that any accumulated depreciation for a disposed asset is appropriately removed from the College's records.

### Depreciation Expense

Once an asset is recorded in AM, ctcLink automatically calculates straight-line depreciation for all assets, based on cost and useful life (**Key Control 2 - AUTOMATED - Valuation**).

### Identified Weaknesses

None.

## **STEP 2: Confirm Key Controls**

**Key Control 1 (Existence, Valuation) - Prior to recording asset information within ctcLink, Sharon Liang (Fiscal Analyst) reviews applicable depreciable asset Purchase Orders and invoices for accuracy.**

We selected Asset ID 10056 for control confirmation, noting that the asset was recorded in ctcLink's Asset Management sub-module (AM) as follows: \$33,057.30, in-service date of 10/17/2023, useful life of 12 years. We obtained invoice 524761 from Jennifer McMillan (Fiscal Reporting Manager). The invoice was dated 9/8/2023, for 1 item (a thyroid uptake system) totaling \$25,650 from vendor Pinestar Technology Inc. Using the invoice, we re-calculated recorded cost for this asset (including ancillary charges of shipping, installation, and tax) to be \$33,057.30; this agrees to amounts per AM without exception. We additionally obtained receiving slips from Jennifer, noting that the equipment was received and installed on 10/17/2023. Finally, we noted that the useful life recorded per AM was 12 years, which is an appropriate designation for medical equipment per SAAM 30.50.10. **No issues noted.**

**Key Control 2 (AUTOMATED - Valuation) - The ctcLink system automatically calculates straight-line depreciation for all assets entered in the Asset Management sub-module, based on cost and useful life.**

## State of Washington

See confirmation of key control at the 'IT Control Testing - Depreciation' step below: [[IT Control Testing - Depreciation](#)].

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at '**MAX**'.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **J.4.PR.G - Community & Tech College Testing - Bellevue**

*Procedure Step:* IT Control Testing - Depreciation

*Prepared By:* JLE, 10/17/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion:
---------------------

#### **Purpose**

To determine whether ctcLink automatically calculates straight-line depreciation for all assets entered in the Asset Management sub-module, based on cost and useful life (**Key Control 2 for ctcLink - Valuation**) was in place and operating effectively and to consider related general IT controls in order to assess control risk.

#### **Conclusion**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period. However, we did not test the operating effectiveness of general IT controls.



# State of Washington

Our understanding and control risk assessment, which incorporates these conclusions, is documented above at: [[Depreciable Capital Assets - Controls](#)].

Testing Strategy:

The following procedures are **required** for all automated key controls for financial and single audits:

## **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

### **Software Calculation:**

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

### **Software Calculation:**

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the*

## State of Washington

*entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

## State of Washington

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP 4: Confirm Key General IT Controls**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

## State of Washington

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

### **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

# State of Washington

## Information Technology Planning Guide

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

**Automated Interfaces:** An interface is a process that moves information from one computer application to another. The interface can occur internally between systems maintained by a single agency, or between systems maintained by different agencies or private companies. The interface can also occur between modules within the same computer application.

The data transferred might be a file consisting of one or more records processed at a later time (batch), or it can be a real-time update. Risk associated with interfaces increases as the number of transactions or the number of other services and systems supported by the interfaced data increases.

Poor design or inadequate oversight can affect the transfer of transaction data among the systems. Interface controls are automated and/or manual processes designed to ensure transmission and processing of information is complete and accurate.

### Manual vs. Automated Interfaces

A "manual interface" is the transfer of data from one system or module to another system or module, initiated and controlled by a user. An example of a manual interface is when customer accounts are downloaded from a utility billing system to be used to perform meter readings. When complete, the file with meter readings may be uploaded and posted to the customer accounts.

An "automated interface" is the transfer of data from one system or module to another system or module that happens automatically based on a schedule, or other predefined criteria. A common example of an automated interface is the payroll module of a system. Typically, a payroll batch is created in the payroll module. Once approved, the batch is automatically sent by the system to the general ledger or other applicable modules, such as accounts payable.

Entities should have reconciliation controls between their various applications regardless of the method used for interfacing.

*Auditors should have determined whether system interfaces are automated as part of the Key Software Applications workpaper. **If not**, ask the following question to determine whether the system interface is manual or automated.*

*Is the data transferred from one system/module to another system/module by a user using an uploading and posting technique? For example, data is pulled from one system into a text file or other format, that is then uploaded into a different system or module by*

## State of Washington

*posting or in an upload feature of the module. If the answer to this question is yes, the interface would be considered "manual" since it is initiated and controlled by manually rather than through an automated process.*

**Edit Checks:** An **edit check** is a programmed routine designed to check input data or processing results for accuracy, compliance, or reasonableness. Types of edit checks include:

Range Checks: ensure that numeric values fall within specified ranges, minimums and/or maximums. For example, ensuring that a capital asset can only be entered as a positive amount, or a purchase order can only be submitted without secondary approval for less than a certain threshold.

Consistency Checks: verify that related data fields are consistent with each other. For example, ensuring that a patient's age matches their date of birth.

Format Checks: validate data formats (for example, dates as MM/DD/YYYY or phone numbers as ###-###-####).

Logical Checks: assess logical relationships between data fields. For instance, verifying that total debits equals total credits in a journal entry.

Duplicate Checks: identify duplicate records or entries. For example, preventing the same invoice from being entered twice.

Cross-Field Checks: compare data across different fields. For instance, ensuring that the start date of a project is before the end date.

Required Field Checks: ensure that mandatory fields are filled out. For instance, making sure that a patient's name and date of birth are provided.

Referential Integrity Checks: validate relationships between data tables. For example, confirming that a vendor number exists in the vendor master file as an active entity.

Outlier Checks: detect extreme or unexpected values. For instance, flagging water meter reading values that are extreme outliers for the customer type or account history.

Pattern Checks: look for specific patterns in data. For example, verifying that email addresses follow a valid format.

Edit checks may result in automatic rejection of a transaction, inability to proceed with a transaction, trigger for additional processing or review, or may simply result in a warning message to the user.

Edit checks may be identified as a key control when they are sufficiently relevant (ie: addressing the risk), precise (ie: able to catch all errors, rather than just being only reasonableness or limit check), and sufficiently strong (ie: prevent invalid transactions, rather than just generating a warning messages). Auditors may identify an individual edit or a group of edit checks together as a key control.

**Computer Generated Reports:** A **computer-generated report** is a report that is created by a computer program. The computer program, also referred to as a report generator or tool, takes data from a data source, such as a database, and displays it in a specified format. The process to generate a report often includes performing calculations on the data, such as summarizing, classifying, etc., before displaying, or can display the calculations on the report.

There are two types of computer-generated reports, pre-programmed and ad-hoc or customized reports.

## State of Washington

Pre-programmed or canned reports are pre-defined reports where criteria and specifications are hard coded in the system. A canned report may allow limited parameters, (month/year, for example), but in general the information that will be displayed is pre-determined. Ad-hoc or customized reports allow the user to drill down and customize what information is displayed on the report based on some allowed criteria, such as account codes, dollar amounts minimum, etc).

In contrast, a **manual report** is one that is created outside the system using data exports or is created ad hoc by a user. An example of a manual report is one that is created by copying data from a data source and pasting the data in an Excel spreadsheet or Word document or Powerpoint presentation where it is then processed further. With manual reports, each time a report is created, the data could be incorrect due to user error, such as not copying all relevant data, or processing errors. Therefore, these types of reports should be understood and tested similar to manual controls.

**Electronic Approvals:** Electronic approvals, electronic signatures and digital signatures are technically different, although often these terms are used interchangeably by entities.

Auditors should have determined whether the electronic approval is an automated control as part of the overall understanding of controls. For automated control purposes, an electronic approval is a software system functionality that:

- Permits a user to approve transaction(s) within the software system

- The system automatically documents, or logs, the data approved by the user and any subsequent manipulation

- The acceptance or rejection of the transaction by the approver will trigger an additional software system process, such as posting of a transaction.

E-mail, scanned-in pictures of signatures, or font-changed signatures, etc. may be part of a control activity but are generally not considered an automated control and are not covered by this testing strategy.

### Electronic Signature vs Digital Signature

An “**electronic signature**” can look like a handwritten signature that has been scanned and then pasted into an electronic document. The reliability of this type of approval is variable. Recommend gaining an understanding of the process used to store and affix the signature to the document and then discuss the process with Team IT Audit before placing reliance on this control.

A “**digital signature**” is a legal signature with a formal certification process that documents who approved the document and ensures the document is not modified after certification. Reliability of this process is very high but has significant technical features. Recommend brainstorm with Team IT Audit before placing reliance on this control.

### **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

# State of Washington

**Statements on Auditing Standards AU-C 315 Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards AU-C 330 Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **STEP 1: Understand Automated Key Control**

**Significant System:** ctcLink

**Key Automated Control:** The ctcLink system automatically calculates straight-line depreciation for all assets entered in the Asset Management sub-module, based on cost and useful life (Valuation).

Our understanding of the overall control is documented as part of our understanding of controls over relevant assertions for Asset Management at the 'Depreciable Capital Assets - Controls' step above: [[Depreciable Capital Assets - Controls](#)].

## **STEP 2: Confirm and Test Automated Key Control**

We confirmed FY24 automated depreciation expense calculation for asset ID 000000010012 (B-Bldg). We obtained the following asset information from Jennifer McMillan (Fiscal Reporting Manager): historical cost (\$450,659.92), useful life (50 years), and acquisition date (6/30/2022). Using this information, we re-calculated FY24 depreciation as follows:  $\$450,659.92 / 50 = \$9,013.20$  annual depreciation. The asset was in service the entirety of FY24, as such, we'd expect that FY24 depreciation expense = \$9,013.20. We ran the following ctcLink query: 'QFS\_AM\_ASSET\_DEPRECIATION' for Bellevue for FY24. We searched the results for asset ID 000000010012, and found that FY24 depreciation was recorded as \$9,013.20 for this asset. Depreciation expense amounts agree without exception, and match auditor expectations. **No issues noted.**

We are not planning to rely on automated controls and therefore do not need to test automated controls; control risk will be assessed at '**MAX**'.

## **STEP 3: Understand General IT Controls**

The College has restricted user access to the Asset Management (AM) ctcLink sub-module; the only individuals which can make changes to depreciation calculations within the system are Jennifer McMillan (Fiscal Reporting & Student Financial Services Manager) and Sharon Liang (Fiscal Analyst) (**General IT Control 1**).



# State of Washington

## **STEP 4: Confirm Key General IT Controls**

### **General IT Control 1 - User access to Asset Management depreciation calculations are restricted to Jennifer McMillan (Fiscal Reporting & Student Financial Services Manager) and Sharon Liang (Fiscal Analyst).**

We reviewed the user role listing ('QFS\_SE\_LISTUSERNAMES\_BY\_ROLE') on 10/17/2024 for depreciation processing and asset entry, noting that user access is restricted to 3 individuals: Jennifer McMillan, Sharon Liang, and Viorika Kazachenko. We specifically note that depreciation processing roles are restricted to Jennifer and Sharon. Viorika has access to asset entry due to her involvement in physical inventory processes.

**No issues noted.**

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at 'MAX'.

## **J.4.PR.G - Community & Tech College Testing - Bellevue**

*Procedure Step:* Depreciable Capital Assets - Testing

*Prepared By:* JLE, 10/14/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion:

### **Purpose**

To determine whether reported capital and infrastructure assets represent real assets, as of the end of the period (Existence).

To determine whether capital and infrastructure assets are reported at properly valued and calculated amounts (Valuation).

### **Conclusion**

We determined that capital and infrastructure assets represent real assets and were reported at properly valued and calculated amounts. **No issues noted.**

Testing Strategy:

The following is a list of **considerations** for testing the existence assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **Nonexistent Assets**

## State of Washington

Review capital asset records to determine whether records meet minimum requirements of BARS [3.3.9.40](#) to positively identify and adequately describe the asset. If asset records are not sufficient, follow up on how the entity is able to identify and track reported assets and consider further audit procedures.

Scan the capital asset list for unusual or unexpected assets or patterns.

*For example: asset descriptions that appear insufficient to identify the asset, asset descriptions that seem strange, assets with a historical cost that doesn't appear to meet the capital asset threshold, assets that are past the end of their service life, assets or asset types that don't appear to belong (based on auditor's understanding of entity activities and area of operation), assets or asset types that the auditor doesn't recognize, attributes that appear unreasonable (historical cost, useful life or scrap value), assets that appear connected to actions noted in planning procedures (impairment, replacement, sale or surplus, transfer), etc.*

Test sampled assets or selected high-risk assets from accounting records for existence by observing them or reviewing documentation.

*Observation for aboveground infrastructure such as roads, bridges or buildings may be by [google maps](#). Documentation for underground assets may consist of maps, system plans approved by regulatory agencies or permits, etc.*

Review the government's records of the latest physical inventory for any identification and follow-up on missing assets or any types of assets or locations that were not covered. Note: review of a government's physical inventory is considered a control test. However, it may be done as a risk assessment procedure to help direct substantive testing, and follow-up on results may result in some substantive evidence.

Trace assets from accounting records to assets listed on the government's insurance policy records. Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

Trace assets from accounting records to operational records (ex: Public Works Department typically tracks assets for maintenance or regulatory reporting purposes). Note: if a complete comparison or reconciliation is made, this test would also provide evidence for the completeness assertion.

For land and buildings, trace parcels and historical cost per the land subsidiary schedules to the County's land (GIS) records to verify ownership. Note: this test also provides evidence for the rights & obligations assertion and - if a complete list is obtained from the County - for the completeness assertion as well.

Compare reported public project completed or in process during the period to the L&I [prevailing wage reporting database](#). Note: since reporting is done by contractors, it would be considered a third-party verification of project existence. We would expect capitalized costs (which include costs incurred by the government as well as contractors) to exceed the contractor's reported costs for most projects. This test also provides evidence for the completeness assertion if traced from the L&I database.

### **Cut-off**

Review supporting documentation to verify dates of any transfers, annexations or donations.

# State of Washington

See the Expenditures | Existence step for testing strategies on cut-off for capitalized expenditures.

## Detail Roll-Up

If manual journal entries are required to update the GL, agree figures per the GL to subsidiary schedules or systems.

Search for manual journal entries that debit (increase) capital or infrastructure assets. Consider testing if any risk indicators are noted.

Reconcile (or review the government's reconciliation) capital expenditures for governmental funds to increases in capital assets. The only anticipated reconciling item would be equipment that is below the capitalization threshold.

Reconcile (or review the government's reconciliation) increases in capital assets to capital purchases and sales per the statement of cash flows for proprietary funds. The only anticipated reconciling item would be donated or contributed assets.

**Over/Invalid Capitalization** - See classification step for testing strategies on improper capitalization upon construction or acquisition, or when determining whether an expense is a maintenance or repair expense or a capitalized improvement.

## Unrecorded Disposals or Impairments

Scan capital asset records for fully depreciated assets and inquire as to the status (disposed, no longer in use, etc.) to ensure all retirements and disposals have been recorded. Evaluate appropriate accounting for any fully depreciated assets remaining in service in accordance with [BARS 3.3.10.130](#).

Identify significant disposals, impairments (due to obsolescence or damage) or contributions per review of minutes and trace to asset records to verify these events were accounted for.

Request a list of insurance claims made during the audit period to identify possible impairments or removed assets, then trace to subsidiary records to verify that the event was properly accounted for.

Identify annexations (through minutes, inquiry or OFM's central annexation tracking system) and trace to supporting documents showing the transfer of assets. Note: this test would also provide evidence for the completeness and rights & obligations assertions.

The following is a list of **considerations** for testing the valuation assertion for capital and infrastructure assets. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## Incorrect Depreciation Calculations

Perform an analytical review of depreciation expense by type of asset for reasonableness.

Re-calculate depreciation expense for a sample of assets or in conjunction with a test of automated controls (if depreciation is automatically calculated by the system). Consider testing the inputs used for the calculation to determine whether they are reasonable and in line with any applicable policies; i.e. useful life, salvage value, etc. Alternatively, test calculations, extensions and footing of subsidiary records if records are maintained on spreadsheets.

Evaluate capital asset policies for componentization or grouping of assets to determine if it has been consistently followed and will result in a rational method of depreciation. See BARS [3.3.10.150](#) for guidance.

## State of Washington

Evaluate estimated useful life and scrap value factors for reasonableness. This test could be done in general (on the government's accounting policies), for selected asset classes or for selected or sampled asset records.

*If testing selected high risk assets, auditors should consider assets that are nearly or fully depreciated (see BARS [3.3.10.130](#)), assets with unusually high or low useful lives for their type, and assets with unusually high scrap values.*

Compare estimated useful lives for assets with replacement schedules / policies and capital budgets.

*We would expect that assets on a regular replacement schedule (such as equipment, vehicles, road surfacing, etc) or that are included for replacement in the capital budget would have estimated useful lives that match the government's replacement plans for the asset.*

Consider whether the date placed in service for assets is reasonable given when the asset begins being used or is substantially complete as this will have an effect on when depreciation begins. See information in BARS [3.3.10.90](#) about when to move a project out of CIP.

### **Impairment**

Check that the measurement method used for write-offs is in accordance with GAAP (GASB 42.12-15). Review or recalculate the portion of historical cost that should be written off for impaired capital assets. *Note: auditor would normally use the same measurement method used by the government unless it the auditor finds it inappropriate for the circumstances or unallowable under GAAP.*

### **Incorrect Historical Cost of Assets**

Trace recorded cost to supporting documentation. *Note: This test would normally be limited to recent additions, since documentation for historical assets has likely passed the records retention period.*

Evaluate the reasonableness of any estimates of the historical cost of capital assets.

Evaluate the reasonableness and support for any estimates of the acquisition value (per GASB 72) of donated capital assets.

### **Conversion to GAAP**

For governments converting to GAAP reporting, examine valuation method for retroactively reported infrastructure assets and verify that the valuation method used is one of the methods prescribed by the County Road Advisory Board.

### **Modified Approach**

Check that infrastructure is being depreciated unless the modified approach is used. If the modified approach is used, verify that the government has met criteria of GASB 34 par 23-26.

### **Allocation**

On the government-wide statement of activities, review allocation of depreciation for capital assets for governmental funds. Depreciation expense

# State of Washington

will be reported as a component of the direct expense shown in the statement of activities. Request spreadsheet for allocation.

Guidance/Criteria:

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

GAAP criteria for reporting capital assets

**[GASB Codification Section 1400 Reporting Capital Assets](#)**

**[GASB Comprehensive Implementation Guide Chapter 7 Basic Financial Statements and Management's Discussion and Analysis, sections 7.9-7.21](#)**

Record of Work Done:

## **Significant Balance and Assertions:**

Governmental Activities - Depreciable Assets (Net of Accumulated Depreciation) - Existence, Valuation

Controls are documented in the "Depreciable Capital Assets - Controls" step. See testing at: [[Depreciable Assets Testing](#)].

## **Substantive tests performed to meet the Existence assertion:**

### *FY24 Asset Additions*

We obtained a workbook titled 'FY24 Summary Capital Asset Report' from Jennifer McMillan (Fiscal Reporting Manager). The workbook tab titled "AM Cost Transactions by BU" detailed all capital asset additions during the year, by asset ID number, as reported per the ctcLink Asset Management submodule. We also obtained general ledger data by running ctcLink query 'QFS\_GL\_SNP\_DETAIL'. We compared total asset additions (by category) per the "AM Cost Transactions" tab of the PBC workbook, to general ledger data obtained by auditors. We excluded CIP additions from our comparison, as CIP does not represent a depreciable asset. Total FY24 asset additions per both reports agreed without exception, totaling \$1,369,331.46.

Using the sampling spreadsheet from the TeamStore, we randomly selected 9 FY24 asset additions for testing, including 1 individually significant asset, for a total of 10 testing selections. For each testing selection, we obtained copies of invoices, purchase orders, and receiving slips from Jennifer. Using this information, we determined whether:

Asset acquisition date, asset description, and recorded cost information traced to invoice and receiving slips.

Asset acquisition date was within FY24

Asset addition meets OFM capitalization criteria per SAAM 30.20

Our testing did not result in any exceptions. **No issues noted.**

# State of Washington

## **Substantive tests performed to meet the Valuation assertion:**

### *FY24 Asset Additions*

We obtained a workbook titled 'FY24 Summary Capital Asset Report' from Jennifer McMillan (Fiscal Reporting Manager). The workbook tab titled 'AM Cost Transactions by BU' detailed all capital asset additions during the year, by asset ID number, as reported per the ctcLink Asset Management submodule. We also obtained general ledger data by running ctcLink query 'QFS\_GL\_SNP\_DETAIL'. We compared total asset additions (by category) per the 'AM Cost Transactions' tab of the PBC workbook, to general ledger data obtained by auditors. We excluded CIP additions from our comparison, as CIP does not represent a depreciable asset. Total FY24 asset additions per both reports agreed without exception, totaling \$1,369,331.46. Using the sampling spreadsheet from the TeamStore, we randomly selected 9 FY24 asset additions for testing, including 1 individually significant asset, for a total of 10 testing selections. For each testing selection, we obtained copies of invoices, purchase orders, and receiving slips from Jennifer. Using this information, we determined whether the asset addition was recorded at cost, and included all ancillary charges. Our testing resulted in one exception, where an asset was overstated by \$922, which projected to a total overstatement of \$9.3K. The misstatement is beneath the floor, both individually and in aggregate. **No issues noted.**

### *FY24 Depreciation Expense*

We analyzed the balance composition of the College's FY24 capital assets, determining that we would focus depreciation expense testing on the 'Building' category of assets, for 82% balance coverage. Jennifer McMillan (Fiscal Reporting Manager) provided a ctcLink query ('QFS\_AM\_ASSET\_COST') detailed asset listing. Jennifer also ran another ctcLink query ('ASSET\_BOOK\_ROWS'), which provided useful life information. She joined these two datasets using VLOOKUP formulas and Excel Pivot tables, and provided results to auditors in a single spreadsheet. We filtered the results of these queries for the 'Building' category, and then filtered again for 'in service' assets. We compared the total of our results, to total 'Building' assets reported per the general ledger (GL detail obtained using query 'QFS\_GL\_SNP\_DETAIL'), noting no exceptions. We then re-calculated FY24 depreciation expense for in-service 'Building' assets, based on PBC acquisition date, historical cost, and useful life. We found a \$213,620 below the floor variance between our re-calculated depreciation expense amounts, and those reported per the College, which we determined to be due to changes in how depreciation was calculated previously in the DirectLine system, versus how it's currently calculated in the ctcLink system. **No issues noted.**

## **J.4.PRG - Community & Tech College Testing - Bellevue**

*Procedure Step:* Charges for Services - Controls

*Prepared By:* SRC, 10/25/2024

*Reviewed By:* CJG, 11/1/2024

# State of Washington

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

**Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted **no** material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

**This workbook template was designed for tuition revenue system control audits at Community Colleges. Contact [Team IT Audit](#) with questions on information or steps contained in this template. The template assumes occurrence and valuation are relevant assertions and that controls over occurrence and valuation will be tested.**

The following procedures are **required** for all relevant systems:

**PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption [RCW 42.56.420](#) for cyber security purposes. The details documented in the record of work and supporting workpapers may qualify for this exemption. Auditors must include this statement in workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

**STEP 1: Control Understanding**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*See the **Client Resource Tab** to reference query tools and year end adjustment information applicable to community and technical colleges. The following are expected controls for and community technical colleges. If sufficient key controls are not in place, the government may be able to demonstrate compensating controls.*

*Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

## State of Washington

*In gaining an understanding of controls, consider the overall understanding of COSO elements as documented in the "Entity-wide COSO Evaluation" step as they relate to this particular system.*

When gaining an understanding of a college's tuition revenue system, the following specific steps should be considered:

### Admissions & Class Registration

Discuss admissions and class registration procedures with department representatives or registrars to gain an understanding of admissions and registration processes and policies. Consider the following:

How is a student's status validated?

How do they assure that a student's status has been accurately posted from Campus Solutions Core to Student Finance (SF)?

### Tuition calculation

The automated tuition calculation processed in the cTclink system has been identified as an automated control. When gaining an understanding of a college's software calculation controls, the following specific steps should be considered:

Gain an understanding of the college's procedures for updating Term Fees, Tuition Groups, Item Types, and Tuition Schedule tables, including any review they perform to ensure the changes made are correct.

Validation of Tuition Calculation at the College - Inquire with college staff to see if they test tuition calculations prior to rolling over term fees, and if so, whether they used the Production College Development (PCD) environment to do so. If they have saved supporting documentation for testing performed, observe testing results to verify that the respective tuition and fee values were actually calculated correctly for each category of mock student tested.

Identify individuals responsible for updating the tuition rates including any users who are authorized to modify the tables or access the screens which have been deemed critical to the tuition revenue calculation process (Term Fees, Tuition Groups, Tuition Calculation, Item Types, and Tuition Schedule)

Consider obtaining the following from college staff when testing calculation of tuition revenue for a sample students:

Approved tuition rates

**Customer Account** reports showing tuition/fee charges on the student accounts

**Customer Academic Information** and **Career Term** data showing the student's status/tuition group

**Enrollment Summary** showing evidence of the classes the student was enrolled in for the selected quarter.

### Tuition payment

Students typically pay tuition and fees by credit card. Credit cards are processed through CyberSource. State and community technical colleges must reconcile payments received, and each individual college establishes their own frequency to complete it. Each cashier closes out



## State of Washington

daily using a batch report from the cTcLink system. The daily batch report may not include daily transactions for EFT's and wires. The following steps should be considered when gaining an understanding of tuition payment:

Discuss cash receipting procedures with department staff and document procedures performed tuition payments paid with the following

- Cash or check
- Credit Card
- ACH/Wire

We expect colleges reconcile credit card payments made through CyberSource. Inquire and document the colleges process of tying credit card payments processed through CyberSource to entries made in the cTcLink system.

Inquire regarding how the college would address variances found when performing reconciliations.

### Posting to the GL

Receipts are posted to the GL through an evening automated batch process. Typically, cash receipts are reconciled daily to bank accounts, and bank account balances reconciled monthly to cTcLink. Consider the following:

- Gain an understanding of the GL posting process, and determine how they validate that their postings are accurate and complete.

- Inquire regarding how the college would know if the GL did not post accurately or completely. It is likely there will be variances in how each college performs their reconciliations, with some using spreadsheets or running queries or customized reports as tools to validate the GL postings.

### Distribution / Allocation to Revenue accounts

Review the procedures the college uses to assure that all tuition revenue payments from GL fund 840 were completely distributed. Consider the following:

Document the process used by the colleges to update/maintain the values in their Tuition Distribution table.

### Transfer to AFRS

Gain an understanding the college's reconciliation process of their cTcLink balances to those posted to AFRS. Consider the following:

Evaluate the college's procedures regarding the year-end closing entries recommended by the State Board (per their "Year End Closing" binder). While the key control is the reconciliation done by the SBCTC, the college still needs to provide oversight and monitoring of the adjustments that are recommended by the SBCTC (colleges should understand what the adjustments are for, that they are correct and properly supported).

*Note:* SBCTC System Accounting Coordinators handle all ctcLink uploads to AFRS. Every month, on AFRS cutoff date, a staff from SBCTC runs a query in ctcLink of all journal entries created. This is a summary level report that is downloaded into an Excel spreadsheet. Staff create two pivot tables; one by funds and amounts, another by general ledgers and amounts. Staff expects the

## State of Washington

pivot table by fund and amount to be zero. Staff then compares the second pivot table to another report, which is generated for the State Auditor's Office (SAO). Both reports are queried from the same database, the one for SAO contains a few more fields. When all the amounts agree, staff is ready to prepare the file to be uploaded into AFRS.

Staff then sort the file by fund, general ledger, and amount. The customization now generates the output files (flat files with transaction codes) and sends them to AFRS. There are usually 1600 to 2200 lines for each college each month. This file is saved as a flat file format and is uploaded into AFRS using the OFM's Financial Toolbox. Sue does a test run in what is known as the SUP environment (copy of previous day's production) to check for any major issues. Staff is able to capture a copy of the flat file and uses that to reconcile between what is in cTcLink and what was transmitted to AFRS. Staff makes any necessary corrections to the AFRS batch and releases the output file to AFRS.

Financial Adjusting Entries – the colleges are directed to use the adjusting entry forms to enter any required cTcLink adjustments, with each suggested adjusting entry denoted in this section. Additional explanations (from the SMARTER system) for each of the suggested adjusting entries are also provided.

SMARTER Queries used to reconcile Finance Sub Modules to the General Ledger. Not all State community and technical colleges use SMARTER Queries, however, use is encouraged by SBCTC.

*Note: Waivers are not included in data reported from cTcLink to AFRS*

Disclosure Forms – Copies of the college's general note disclosures and supporting documentation.

Payable/Receivable reporting reflecting any payables ("due to") and receivable ("due from") transactions with other state agencies.

*Note: Some reports and queries used by colleges may be built in-house and may be used alongside SMARTER queries that have been built by SBCTC. If the college does not have a good understanding of the reconciliation process done by the SBCTC then the auditor may want to consider reviewing the year-end adjustments for material errors. For example, the auditor could request the Year End Closing documentation from the State community or technical college and review it to determine the types of adjusting entries and exception items noted by SBCTC.*

### **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

### **Step 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a*

## State of Washington

*control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4.A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.*

### **STEP 4: Test Controls**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

***Since key controls for Tuition Revenue are automated, Auditors should add the "IT Control Testing - Tuition Calculation" step available in the Store to document automated and general control testing.***

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of COSO elements. In doing so, all of the following specific determinations must be documented:*

- A. Key controls – including personnel who affect the application of the control – have not changed since they were last tested. Automated controls should be tested the first year that colleges use the cTclink system.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2021, this work could potentially be relied upon for both the periods ending 2022 and 2023.*

### **Step 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

### **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security

# State of Washington

require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

## **SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

Record of Work Done:

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Education - Higher Education Charges for Services - Occurrence, Valuation

Higher Education Special Revenue - Charges for Services - Occurrence, Valuation

See lead sheet here: [[Lead Sheet](#)]

## **STEP 1: Gain an Understanding of Internal Controls**

We spoke with Jennifer Mcmillan, Finance Manager, and Roselle Hay, Accounting Manager, on September 18, 2024 regarding controls over student tuition and fees in the ctcLink system.

Software used by community colleges to generate tuition revenue was developed and is maintained by State Board of Community and Technical Colleges (SBCTC). Student information is captured in the ctcLink system in Campus Solutions (CS) Core module. Tuition is **automatically calculated** and applied to student accounts within the Student Financials (SF) Module based on their class registration for the quarter. The rates and codes used in the tuition calculation process reside within several key system tables, which are maintained by SBCTC. Tuition and fee rate tables are updated annually and posted on the [SBCTC website](#).

# State of Washington

## **Admissions & Class Registration**

The Admissions office processes the student applications within Campus Solutions module. When the first billing record is generated for the student (i.e., for admissions or testing fees), an account is created for the student in the Campus Solutions Core module.

Students can register online through their ctcLink account or in person at the Admissions office. Critical information associated with tuition revenue is captured at this point regarding the student's status (i.e. resident, non-resident, veteran, etc.), and this data is posted to the Campus Solutions Core module.

Students typically register for classes on-line, but they can also do so in person. Classes are defined within the Campus Solutions Core module. The information captured in Campus Solutions Core during registration will be used in calculating the amount of tuition and associated fees owed by each student.

A student's tuition and fee liability is recorded in the Campus Solutions Core database when students register for classes, but revenue will not be recognized in the GL until a journal is created in Campus Solutions Core and automatically sent to Student Financials via nightly batch.

## **Tuition Calculation**

Item Types:

Item types are the basic work unit of the Student Financial application in ctcLink, they work like a fee code for charging tuition. Each item type defines and describes a unique action and has an associated fee table which breaks down the charge per credit for that item type. The system uses item types to transfer student account information to the general ledger based on the set up. SBCTC maintains item types for the college and has a ticketing system for any requested updates, changes or additions to the item type list. There are unique item types for tuition, different types of fees, payments, and financial aid, which are grouped by category. Jennifer let us know that only the SBCTC can approve, create, or make changes to item types GL distribution in the system.

The ctcLink system automatically calculates tuition for all students based their class registration and the tuition rate and fee tables set by the State Board (**Key Control 1- Valuation, AUTOMATED**). The result of this calculation is recorded in the SF database and will be netted against any financial aid awards or fee waivers in determining each student's final liability. The system is also programmed to split the charges between funds such as Operating, Building, and Services and Activities, all of which receive a pre-set percentage of the charges.

## **Financial Aid, Scholarships, Waivers and Scholarship Allowance (Tuition Discount Methodology)**

The College offers Tuition Discounts through Financial Aid, Scholarships, and Waivers.

### **Waivers:**

Waivers are regulated by SBCTC, who decides which waivers colleges are required to offer and which ones are optional. The Bellevue College

## State of Washington

Board of Trustees approves optional waivers, as well as the amount of the waiver and what the waiver affects (tuition or fees). Each waiver has unique guidelines. The College offers tuition and fee waivers for specific groups of students:

- Military and Service Related Waivers
- Space Available Waivers (Senior Citizens and State Employees)
- Nonresident Tuition Waivers

SBCTC configures the waivers to reduce the balance of the student's account by applying it like a payment. Waivers are applied quarterly, and the payment flows to the GL and hits a contra account. The chart strings it follows depends on if the waiver is paying for fees or tuition. During the first years of cTcLink implementation, Jennifer has been periodically reviewing waiver activity to ensure the payments are hitting the correct accounts.

### **Financial Aid and Scholarships:**

Students can apply for Financial Aid (FA) and Scholarships through the designated module in the Campus Solutions pillar of cTcLink. Once the student has been awarded FA, the data flows from the FA Module to the student's account. Like a Waiver, the FA disbursements are programmed to act like a payment on the student's account. Disbursements can be deposited on a weekly basis and are recorded in a journal entry overnight.

### **Scholarship Allowance (NACUBO)**

At the end of the year when the College prepares their financial statements, they perform a Tuition Waiver calculation in compliance with NACUBO (National Association of College and University Business Officers) standards. SBCTC provides the template to the College as an excel workbook. Jennifer McMillan, Finance Manager, completes the template using data pulled from cTcLink. The total "tuition waiver" is meant to represent the total amount of discounts provided to students throughout the year from both Federal sources and State, including non-monetary discounts which are assigned an estimated value. The workbook currently follows NACUBO's "Alternative Method". The calculated amount will reduce the reported revenue from student tuition and fees on the financial statements. The workbook was not yet completed for FY24 at the time of the audit, however, we were provided with the workbook for FY23 and noted that the scholarship allowance per NACUBO was valued at \$8,765,451 which was reduced by the amount of tuition waivers already booked as a reduction of tuition (\$2,981,861). The total reduced scholarship expense inserted into the notes of financial statements was reported as \$5,783,589.

### **Tuition payment**

Deadlines for tuition payments are posted on the College's website. Students are not permitted to start class until they have paid in full, have a payment plan set up through Nelnet, or have been approved for FA are awaiting disbursements. Tuition can be paid online through Cybersource or in person at the Cashier's office. Payments are captured by the cTcLink receipting module and recorded in the Student Financials (SF) module. Cybersource payments are integrated and post to the student's account immediately, cash and checks are processed and post 1-2 days later. Each college may use a tuition installment program allowing designated students to pay tuition in several installments. Outstanding balances are retained only in Student Financials (SF) and posted to the GL when payment is made. A student's tuition and fee liability is recorded in the SF

## State of Washington

module database when they register for classes, and revenue is recognized in the GL at the time of registration.

Cashiers receive payments and code receipts by student which automatically codes to item types set up in the system. Students can either pay at the office, or mail payments into a kiosk electronic that is collected and entered in the system by cashiers. If payment is not received by the payment deadlines set by the college (prior to start- registrations staff runs this office), the student is dropped. Registration staff identifies dropped students and gives cashiering department a list.

### **Posting to the GL**

Tuition revenue is recognized as a receivable when a student's enrollment is complete and student status is validated. Upon completion of the student's enrollment in classes for the term, a journal entry is created in Campus Solutions (CS) and sent to Finance via nightly an automated nightly batch process. If a student drops a course, the receivable is reversed.

Cash receipts are posted to the GL through the nightly batch process. If there are posting problems, the system notifies the user that the batch did not post. Corrections are made through a batch edit screen, and the corrected batch is remitted. Tuition payments result in revenue being posted to Fund 840 under the source codes 0424 (tuition) and 0430 & 0431 (supplemental fees).

Tuition payments result in revenue being posted to each fund associated with tuition (060, 149, 522, 561, 860) under the tuition GL Account codes: 4000020, 4000030, 4000040, 4000065. Note that Spring/Summer pre-payments for Fall Quarter tuition (deferred revenue) are moved to a deferred revenue GL Account 2040010 at FYE. This entry is reversed on July 1 of the next fiscal year.

### **Reconciliation**

Student financials batches are reconciled to the GL on a regular basis by a Fiscal Analyst 5 (FA5), though the college let us know that their FA5 position is currently being recruited. They do daily cash reconciliations and use system reports and queries to identify any discrepancies between the student financials module and the general ledger. An electronic report is downloaded from the bank each month that includes all of the check deposits, credit card payments and refunds for the prior month. An FA5 Accountant in Finance performs a bank reconciliation to ensure all funds received reconcile to the bank and are posted to the GL. Also, the FA5 Accountant in Finance performs a SF module to GL reconciliation to ensure all funds received are posted to the GL (**Key Control 2 - Occurrence**).

### **Distribution / Allocation to Revenue accounts**

An automated monthly process is run in ctcLink to allocate tuition revenue payments from GL fund 840 to the funds below. With the exception of Service & Activities fees (set by the Local Board of Trustees), the individual fund distribution percentages are determined by the Legislature. The local college manually posts and retains these percentages in the Tuition Schedule.

060 (Building fee portion; remitted back to the State)

149 (Operating fee portion)

## State of Washington

522 (Services & Activities portion)  
561 (Comm/Tech College Innovation portion)  
860 (Institutional Financial Aid portion)

Additionally, at year end, the Finance Manager reviews the amount collected for the upcoming Summer and Fall quarters and moves the tuition and related receivables by journal entry to the deferred revenue account to be recognized in the correct fiscal year (**Key Control 3 - Occurrence**).

### **Transfer to AFRS**

Bellevue College does not upload data into AFRS. SBCTC is responsible for pulling all relevant data from cTcLink and getting it into AFRS using the process as follows: System Accounting Coordinator handles all ctcLink uploads to AFRS. Every month, on the AFRS cutoff date, runs a query in ctcLink of all journal entries created. This is a summary level report that is downloaded into an Excel spreadsheet. The Coordinator then creates two pivot tables; one by funds and amounts, another by general ledgers and amounts. Staff expects the pivot table by fund and amount to be zero. Staff then compare the second pivot table to another report, which is generated for the State Auditor's Office (SAO). Both reports are queried from the same database, the one for SAO contains a few more fields. When all the amounts agree, staff prepare the file to be uploaded into AFRS.

Staff then sorts the file by fund, general ledger, and amount. The customization now generates the output files (flat files with transaction codes) and sends them to AFRS similar to how it is done in the Legacy system. There are usually 1600 to 2200 lines for each college each month. This file is saved as a flat file format and is uploaded into AFRS using the OFM's Financial Toolbox. A test run in what is known as the SUP environment (copy of previous day's production) is then used to check for any major issues. Staff is then able to capture a copy of the flat file and uses that to reconcile between what is in ctcLink and what was transmitted to AFRS. Staff makes any necessary corrections to the AFRS batch and releases the output file to AFRS.

### **Key Controls:**

**Key Control 1 – AUTOMATED (Valuation)** - The ctcLink system automatically calculates tuition for students when they register for classes based on their residency, division, registration, and the tuition rate and fee tables set by the State Board.

**Key Control 2 - (Occurrence)** - Receipted tuition payments are reconciled to the general ledger on a daily basis, which are then compiled to perform a monthly reconciliation, based on the payment receipt method. Also, the FA5 Accountant in Finance performs a SF module to GL reconciliation to ensure all funds received are posted to the GL.

**Key Control 3 - (Occurrence)** - At year end, the Finance Manager reviews the amount collected for the upcoming Summer and Fall quarters and moves the tuition and related receivables by journal entry to the deferred revenue account to be recognized in the correct fiscal year.

## **STEP 2: Confirm Key Controls**



## State of Washington

**Key Control 1 – AUTOMATED ( Valuation) - The ctcLink system automatically calculates tuition for students when they register for classes based on their residency, division, registration, and the tuition rate and fee tables set by the State Board.**

We confirmed the automated control at [Community & Tech College Testing - Bellevue] and tested it here: [Charges for Services Testing - CONFIDENTIAL] - *No issues noted.*

**Key Control 2 - (Occurrence) - Receipted tuition payments are reconciled to the general ledger on a daily basis, which are then compiled to perform a monthly reconciliation, based on the payment receipt method. Also, the FA5 Accountant in Finance performs a SF module to GL reconciliation to ensure all funds received are posted to the GL.**

We met with Jennifer McMillan on September 23, 2024 over Teams, and she walked us through her many types of reconciliations of the SF module in ctcLink to ensure the information is posted to the general ledger accurately and completely. Jennifer demonstrated to us how she performs a rolling reconciliation on a daily basis by pulling transaction by transaction data from Cybersource (Student ID, amount paid, and date paid) and pulling information from student accounts which lists the amount they we billed. The info is entered into the Workbook which is set up to compare the reports calculate the difference in a spreadsheet. At the end of the month, these daily reconciliations are compiled and used for the monthly reconciliation. During our Control walk-through, we focused on the "Book to Bank" Workbook for the month of June 2024 which holds tabs for the GL Payments in Transit by type, Deposits in Transit by type, Legacy Checks, and Daily Deposits by type. These feed into another tab that compares these totals with a tab that holds the current bank statement and highlights any differences between the two tabs. There is also a tab set aside as a placeholder for outstanding payments that have not cleared by the end of the month. Jennifer explained that the deposits received can be from many sources including Nelnet (payment plans), Bankmobile refunds (student aid), online credit card (Cybersource) payments, but the deposits all have different timing and can be received a few days from the collection date. The daily deposit totals are downloaded from bank reports and documented on another tab of the spreadsheet. Jennifer has a formula that combines the types of deposits and sorts them by date. Jennifer runs pivot tables from SF and GL reports to compare the totals by day - She uses the CTC All Cashier Receipts query and the GL account analysis query to compare item type totals by day and month. Jennifer noted that the Workbook is set up to keep everything balanced, and she is diligent about reviewing the it daily to make sure everything is matching.

There was also a column to identify final differences that need to be researched and corrected if necessary. Jennifer let us know that the Treasury module in the General ledger Finance pillar does not automatically post all SF transactions so "external Transactions" must be created in the treasury module using the summarized daily SF reports in order to tie out the final monthly bank reconciliations.

Jennifer also reconciles SF payments by tender type which feeds into the main reconciliation. She uses the E214 report form the SF module and compares it with the Key bank merchant log by month.

We noted that the recon was initialized on 6/30/24, and the status of the recon is "Finalized". There was a \$20 difference between Bank and Book, which was reconciled to "In-process errors". The reconciliation was signed by Jennifer on 8/29/24 and reviewed by Ty Bergstrom on the same day.

## State of Washington

*We determined that the finance department is performing regular reconciliations of the SF module to the General ledger to ensure that differences are identified and corrected, and the information reported in the general ledger is accurate and complete. No issues noted.*

**Key Control 3 - (Occurrence) - At year end, the Finance Manager reviews the amount collected for the upcoming Summer and Fall quarters and moves the tuition and related receivables by journal entry to the deferred revenue account to be recognized in the correct fiscal year.**

We requested the support for the journal entry related to unearned revenue collected during FY24 for summer and fall tuition of the next fiscal year. We were provided with three spreadsheets:

The first one was titled "Unearned Revenue- AR offset FY24" which was support for Journal entry 479645, dated 6/30/2024 during period 12. It contained a pivot table for accounts 1011010 (SF Tuition receivable) and 1011020 (SF Fees Receivable) from a detail report on the next tab.

The pivot table sorted the amounts from the two receivable accounts by fund and totaled them to \$9,524,497.30.

There was another pivot table from the report below the first one that totaled the information above by department.

Next to this was detail of debits to account 2040010 (unearned revenue ST) and credits to be made to the receivable accounts by department.

The next spreadsheet was titled "Unearned Revenue - Net Summary FY24" which contained pivot tables of the information above as applied to the revenue accounts and the net result of journal entry 479645 by fund to each revenue account.

The next spreadsheet was titled "Unearned Revenue FY24" and it contained pivot tables from the cTclink query QCS\_SF\_ACCTG\_LN\_TERM\_REV\_SRC. The report detailed SF Journals posted to GL accounts by fund, department, account, term, and item type by date for unit 080. The pivot tables summarized the information from the report by fund and account.

Jennifer also provided us with a SBCTC Memorandum title "Unearned Revenue/Accounts Receivable/Allowance for Doubtful Accounts" which details the process of recording and adjusting for those accounts.

*We determined that the college is analyzing general ledger accounts and moving amounts collected for the next fiscal year to unearned revenue to ensure that reported revenues were posted to the correct fiscal year. No issues noted.*

### **STEP 3: Preliminary Control Risk Assessment**

**MAX - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.**

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

# State of Washington

## **STEP 5: Final Control Risk Assessment**

**MAX - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.**

### **J.4.PRg - Community & Tech College Testing - Bellevue**

*Procedure Step:* IT Control Testing - Charges for Services

*Prepared By:* SRC, 10/24/2024

*Reviewed By:* CJG, 11/1/2024

#### **Purpose/Conclusion:**

##### **Purpose:**

To determine whether the automated control **(key control #1 for ctclink - Valuation)** was in place and operating effectively and to consider related general IT controls in order to assess control risk.

##### **Conclusion:**

Based on our understanding and test results, we concluded that the automated control **was** in place and operating effectively.

Based on our understanding, related general IT controls **were** in place and adequately designed to ensure that the control operated consistently during the audit period.

Our understanding and control risk assessment, which incorporates these conclusions, is documented at [\[Community & Tech College Testing - Bellevue\]](#).

#### **Testing Strategy:**

The following procedures are **required** for all automated key controls for financial and single audits:

##### **STEP 1: Understand Automated Key Control**

Gain an understanding of the automated key control. The understanding can either be documented in the control system step or could be documented here in this step. Auditors should consider the following aspects of the automated control when gaining an understanding:

# State of Washington

## Software Calculation:

Is there written documentation of the calculation, and/or the source rates and factors used in the calculation?

*We would expect written documentation that defines the calculation and is an official, approved source for the formulas, rates and factors. This may be an approved policy or could be system documentation.*

What formulas are used to make the calculation?

What values or factors are used to make the calculation? For example:

- Rate tables used by the calculation
- Profile fields (i.e., applicable transaction types)
- Programmed/set formulas and/or values
- Constraints (i.e., effective date, minimums/maximums, etc.)

How is the calculation triggered or initiated?

How is the calculation recorded in the accounting system (or used in an end result)?

## **STEP 2: Confirm and Test Automated Key Control**

Confirm and test the automated control. To test the automated control, consider the following procedures:

## Software Calculation:

Re-perform the calculation for selected transactions.

*Auditors would NOT normally use sampling for automated controls. Instead, auditors should judgmentally select one instance of each significant variation of the calculation. If the number of potential variations is large, auditors would judgmentally select based on risk factors (for example, the most common scenarios, or scenarios associated with identified risks, or scenarios that are not addressed by the entity's testing procedures).*

*In some cases, it may be possible for the auditor to reperform the calculation for the entire population.*

If any rate tables or values were updated during the period, view the current values (by observing the rate table or values in an admin menu or from a printed system report) and compare to approved sources.

*If no updates were made or there are only a few values, this risk could be addressed by re-performing the calculation. However, if source rate tables or values are large or complex, it may be more efficient to test these values directly than to recalculate a larger number of transactions.*

## State of Washington

Consider the use of analytical procedures such as trends or descriptive statistics on the population (like average, minimum and maximum values, or a graph of values across the population) and follow up on any unexpected values or trends. *Analytical procedures would normally also count as a substantive test.*

### **STEP 3: Understand General IT Controls**

Gain an understanding of the general IT controls that support the continued proper operation of the automated control. Identify key general IT controls and note any control weaknesses. Auditors should consider the following aspects of general IT controls when gaining an understanding:

#### **Software Calculation:**

Inquire if the entity has experienced any errors or irregularities with the calculation. Also how often changes are made to the calculation, and how many changes (if any) were made during the year.

How can the software calculation (formulas, rates/values, settings/configurations) be changed or customized?

*Software calculations will usually have one or more administrative menus that allow the government to modify rate tables or other calculation values, or to configure the calculation or apply settings.*

*In other cases, software calculation formulas and/or values may be hard-coded into the system and require programmers to make the changes. If the government has access to source code, then it needs internal procedures for program changes. If the program is controlled by vendors, we would expect program change procedures and expectations to be included in the contract.*

What are the procedures to authorize and make program changes or configuration/setting changes to the software calculation?

*Except for the most simple situations, we would normally expect program change procedures to be written. Best practices for change management procedures include: (1) assigning responsibility for authorizing changes and executing changes, (2) specifying communication for requested changes and completed changes, and (3) testing or acceptance procedures to review and verify changes.*

What are the procedures to test that program changes are properly working?

*If utilizing a test environment, there should be controls to ensure that the live environment is updated and is consistent with the live production environment. As management is responsible for the accuracy of their automated controls (i.e., in the live environment), we would expect there to be a procedure to confirm each key automated control once it is in the live environment. This could be manually re-performing the calculation, reviewing reports against known expectations, etc.*

How are program changes or configuration/setting changes monitored or reviewed?

*Except for the most simple situations, we would normally expect a secondary review of all changes. Review could entail periodically*

## State of Washington

*checking a change log (if the system logs changes), independent verification of changes (such as a secondary look at updated rate tables or admin menu after changes were applied), independent system testing, or reviewing change and/or test documentation on a periodic or per-change basis.*

If the entity relies on general controls performed by a third-party, determine whether they have a SOC report, contract, or other documentation that describes vendor responsibilities and any complementary user controls expected to be performed by the entity.

*For example, local governments may not have access to change programming, but they may be responsible for patch management, master table data, and/or configurations.*

### **STEP**

Confirm your understanding of key general IT controls to determine whether they have been placed in operation (*whether the entity has actually implemented key controls*).

### **STEP 5: Test Key General IT Controls**

Document whether general IT controls will be tested. Option 1 would result in control risk at MAX for the automated control. Either option 2 or 3 is necessary in order to set control risk at LOW. If general IT controls are tested, consider the following procedures:

#### **Software Calculation:**

If program changes or setting/configuration changes are logged, review the change log to verify the population of changes for the year.

*Verification that no changes were made, along with the auditor's evaluation that no changes are expected, would normally be sufficient evidence to conclude that no further testing of general IT controls is necessary.*

Review programming change documentation or the entity's test documentation for selected or sampled changes. Alternatively, re-performing the calculation may also provide this evidence if the re-performance tests address all states of the calculation during the period.

If limited access to the administrative menu is key (and changes are not logged), request a user access report and verify that access is limited to only authorized personnel.

If the entity relies on a SOC report for general controls performed by a third-party, review the report applicable to the audit period using the [SOC Report Reliance](#) workpaper in the Store.

### **STEP 6: Final Control Risk**

Evaluate the results and document a final control risk assessment in the control system step. Consider whether any deficiencies identified with either the automated control or related general IT controls represent material weaknesses or significant deficiencies.

# State of Washington

*Note: general IT control deficiencies do not necessarily mean the automated control is not properly functioning. General IT control deficiencies would normally be considered a significant deficiency or material weakness only if it caused an issue with the compliance requirement or assertion.*

## **Recommendation Review Requirement**

IT Security related information is considered category 3 data protected by Public Request Exemption RCW 42.56.420. Issues related to IT Security require the following special handling:

[Instructions](#) are located in Team IT Audit's System's Sharepoint page.

Details of IT Security related issues should NOT be included in any emails or helpdesks.

Exit, ML and Findings should be separately communicated in an IT Security Results Document.

Findings will be referenced, but not included in the audit report.

All IT security-related recommendations must be reviewed by [Team IT Audit](#).

Template language for common IT related recommendations can be found in [ARS Part 5 Chapter 8](#).

## **PUBLIC REQUEST EXEMPTION**

Some IT related information is protected by Public Request Exemption RCW 42.56.420 for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. If so, auditors must include this statement in the record of work done and any related workpapers: **"This record contains information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited "**.

Guidance/Criteria:
--------------------

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

## **Information Technology Planning Guide**

Auditors may contact [Team IT Audit](#) with any testing strategy or control assessment questions or to request assistance from an IT Specialist.

**Software Calculation:** A **software calculation control** exists when the value of a transaction is determined by a software application. This process can be a key control when the entity relies on the system to generate calculations correctly to determine the amount of transactions (i.e., summarizing/account code allocation to post to general ledger, calculate student, utility, other charges, etc.).

## **AUDIT CRITERIA**

# State of Washington

Key criteria that auditors will likely use when testing this area.

**Statements on Auditing Standards AU-C 315 Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement** - paragraphs .A106-.A109 describe general and application controls and how they relate to audit risks

**Statements on Auditing Standards AU-C 330 Performaing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained** - paragraphs .10b and .A33-.A34 describe requirements and guidance for testing indirect controls in conjunction with tests of controls, that is, testing key general controls in conjunction with a test of a key automated control

Record of Work Done.

**This record may contain information considered exempt from public disclosure under RCW 42.56.420 of the Public Records Act. As such, distribution of this record is limited.**

## **STEP 1: Understand Automated Key Control**

**Significant System:** Tuition Revenue

**Key Automated Control:** The ctcLink system automatically calculates tuition for students when they register for classes based on their residency, division, registration, and the tuition rate and fee tables set by the State Board (Valuation).

A high level understanding of the automated control is documented as part of our overall understanding of controls over relevant assertions for the ctcLink system above at the "Charges for Services-Controls" step.

## **STEP 2: Confirm and Test Automated Key Control:**

We confirmed and tested the key automated control as follows, to determine whether the automated controls can be relied upon:

We recalculated a sample of ctcLink calculated student tuition & fees amounts on student accounts at: [Charges for Services Testing - CONFIDENTIAL]. *No issues noted.*

## **STEP 3: Understand General IT Controls**

The tuition revenue calculation processing resides within a third-party vendor application system, which cannot be modified by system users. The only way for college users to affect the calculation is through edits to associated data tables and screens and many of those tables are restricted to modification by State Board at the college level.

We met with Jennifer McMillan, Finance Manager, via Teams on October 11, 2024 to discuss General IT Controls around Tuition rate and calculation input and adjustments. Jennifer explained that SBCTC took over all duties regarding tuition data input to the ctcLink system sometime within FY24. Jennifer runs a query in ctcLink of Bellevue College employees who still have access to make changes. She maintains a list in spreadsheet called SACR Security Roles for Term Fee Updates (**General IT Control 1**). Employees must work with Security Administration at the College to be added to this list. However, there have been no instances of a College employee needing to go into the system to make changes since SBCTC took over that role. Instead, employees can submit a ticket through Solar Winds if there is an issue, and the Board will update



# State of Washington

ctcLink accordingly.

## **STEP 4: Confirm Key General IT Controls**

**General IT Control 1 - User access at the college level is limited to 3 employees and is monitored by Jennifer McMillan, Finance Manager, in the SACR Security System.**

During our meeting with Jennifer McMillan on October 11, 2024 we viewed a screenshare of authorizations in the security system. We also obtained the SACR Security Roles for Term Fee Updates spreadsheet that Jennifer maintains which contains a list of employees who have Student Financial Local Configuration access and a list of employees who have Student Financial Charges and Fees Configuration access. For the Charges and Fees list, there are three Bellevue College employees with access, and Jennifer was able to explain their roles and why access was granted to those individuals. The rest of the list contained 28 members of the Board who share the same privileges. ***No issues noted.***

## **STEP 5: Test Key General IT Controls**

Not applicable - we are not planning to rely on automated controls and therefore do not need to test general controls; control risk will be assessed at **MAX**.

## **J.4.PRG - Community & Tech College Testing - Bellevue**

*Procedure Step:* Charges for Services - Testing

*Prepared By:* SRC, 10/28/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion.
---------------------

### **Purpose:**

To determine whether reported revenues represent actual amounts relating to the period (Occurrence).

To determine whether revenues were reported at properly valued or calculated amounts (Valuation).

### **Conclusion:**

We determined revenues were reported at properly valued or calculated amounts (Valuation). We determined reported revenues represent actual amounts relating to the period (Occurrence). ***No issues noted.***

# State of Washington

## Testing Strategy:

The following is a list of **considerations** for testing the occurrence assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

For revenues received from the State Treasurer, trace reported amounts to the State Treasurer confirmations available in LGCS.

Confirm intergovernmental revenues with the other government or grantor or by reviewing appropriate correspondence.

Trace selected or sampled revenues from the GL to supporting billings or subsequent receipts.

If revenue is receipted into a specific clearing account, or if third-party lockbox or receipting services are used, compare recorded revenue to a sum of monthly totals from bank, lockbox or service organization reports.

Develop sufficiently precise expectations for a substantive analytical to compare to reported revenue amounts.

Search for manual journal entries that credit (increase) revenues. Consider testing if any risk indicators are noted.

### **Cut-Off / Revenue Recognition**

Test a sample of underlying transactions to verify the revenue was recorded for the proper period. Note: transactions at the beginning and end of the period would generally be considered at highest risk of being improperly recorded in the current period.

If revenue is billed at a constant rate, calculate an expectation based on the average monthly billing or re-calculate the year-end accrual journal entry and compare to the reported receivable.

Evaluate revenue recognition against GAAP criteria for selected transactions or revenue streams.

### **Interfund Revenues**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

### **Detail Roll-up**

Compare year-end totals from general ledger to subsidiary software modules for selected revenues.

Review the government's reconciliation of general ledger to subsidiary ledgers.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks. For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

The following is a list of **considerations** for testing the valuation assertion for revenues. Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

### **- Calculation**

## State of Washington

Recalculate billed revenues on a check (one of each variation), CAATS or sample basis.  
For large populations of standard billings, perform CAATS tests to identify unexpected or outlier transactions for further review.  
Review related-party transactions to determine whether revenue transactions were correctly calculated.

### Realizable Value

Re-calculate a sample or selection of billings. If billings are calculated by software, the auditor could test and substantiate the automated control and also consider any risks associated with manual inputs used by software.

Evaluate the entity's calculation of the allowance amount for reasonableness. This evaluation should include comparing the entity's estimate to the entity's actual historical experience of collecting or writing-off receivables.

Trace the amount of bad debt approved by the governing body (per minutes) to reductions of receivables and bad debt expense to verify it was properly accounted for. *Note: approvals may be slightly more, as customers may pay after the bad debt has been approved but before it is written off.*

### Estimation / Recognition

Review calculation and support for assumptions of any estimated revenues.

Accounting research to verify that revenues were reported in conformity with revenue recognition policies reported in the financial statement notes.

Guidance/Criteria.:

Record of Work Done.:

### **Significant Balances and Assertions:**

Governmental Activities - Education - Higher Education Charges for Services - Occurrence, Valuation  
Higher Education Special Revenue - Charges for Services - Occurrence, Valuation

Controls are documented in the "Charges for Services - Controls" step.

### **Testing Population:**

We requested a list of all students by quarter from FY24 with amounts charged for tuition and fees. Jennifer McMillan, Finance Manager, provided us with a pivot table and raw data from cTcLink query (CTC\_SF\_ACCTNG\_LN\_BY\_TERM); containing student transaction level data (by student, quarter and GL account). We ran cTcLink query QFS\_GL\_ACCT\_ANALYSIS and filtered for accounts 4000010, 4000020, 4000030, 4000040, 4000050, which are used for Student Tuition revenue. We were able to tie this to the data provided by Jennifer, filtered for the same accounts.

## State of Washington

There was no variance, and we determined our population complete for testing.

We used the random number generation formula to randomly select students by term. Our sample contained 7 students from Summer 2023, 9 students from Fall 2023, 6 students from Winter 2024, and 8 students from Spring 2024, for a total of 30 students.

### **Substantive tests performed to meet the Occurrence assertion:**

We reviewed the account statement and schedule for each student and noted the quarter and date paid for tuition and fee charges were recorded in the correct period. See ctcLink tuition revenue testing at "FS Substantive Sample" at: [[Charges for Services Testing - CONFIDENTIAL](#)]. ***No issues noted.***

### **Substantive tests performed to meet the Valuation assertion:**

We recalculated tuition and fee amounts using the published tuition and fee amounts listed on the Bellevue College web site, and tuition rate workbooks provided by Jennifer, to ensure tuition and fee charges were correctly calculated on student accounts. Some charges did not initially tie out, and we had to request more information from the College. The inconsistencies were due to the student being a running start student where the tuition was covered by a running start waiver up to a certain amount of credits, the student dropping a course during the 50% refund period, or the student being classified as International where their tuition was listed as a Mandatory Fee. The college provided additional support as requested and all students tied out with no variances noted. See Valuation testing in the "TESTS -VALUATION AND IT CONTROL" tab at: [[Charges for Services Testing - CONFIDENTIAL](#)]. ***No issues noted.***

### **J.4.PRG - Community & Tech College Testing - Bellevue**

*Procedure Step:* Education Expenses - Controls

*Prepared By:* JLE, 10/17/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion.*
----------------------

### **Purpose**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

### **Conclusion**

We have gained an understanding of internal controls and assessed control risk at '**MAX**'. Therefore, we **will not** place reliance on controls. Our

## State of Washington

understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted the following control weakness, which we **do not** consider to represent a significant deficiency or material weakness:

**Control Weakness 1** - We identified four individuals with unauthorized budget combo code user roles within the ctcLink system. **See issue at: [V: Bellevue College Confidential System User Access IT Controls].**

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

### **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

### **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers,*

## State of Washington

*reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

### **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it*

## State of Washington

*would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

# State of Washington

Record of Work Done:

## **Significant Balances and Assertions**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities- Education - Higher Education Expenses- Completeness, Classification

Higher Education Special Revenue - Charges for Expenses - Completeness, Classification

See lead sheet at: [[Lead Sheet](#)]

## **STEP 1: Gain an Understanding of Internal Controls**

We gained an understanding of internal controls over education expenses via Teams meeting with the following individuals:

Jennifer McMillan (Fiscal Reporting & Student Financial Services Manager) - meeting for general disbursements on 9/11/2024, meeting for payroll on 9/17/2024

Roselle Hay (Accounting Manager) - meeting for general disbursements on 9/11/2024

Olga Krichevskaya (Payroll Manager) - meeting for payroll on 9/12/2024

Sung Moon (Grants and Contracts Manager) - meeting for payroll on 9/17/2024

## **General Disbursements**

### *Background Information*

Purchases are initiated by decentralized departments across the College via electronic requisition requests in ctcLink. The requisition request triggers a notification to the centralized Purchasing department, which is tasked with generating Purchase Orders (PO) and ensuring that proper approvals are received for the expenditure. The Accounts Payable (AP) department becomes aware of outstanding POs in a variety of ways: most commonly, various College departments will submit POs with attached invoices to AP. AP also receives invoices directly from vendors via their departmental email inbox - when this occurs, AP contacts the applicable department to request a copy of the PO. Rarely, AP is unaware of an outstanding invoice until it becomes past due, at which point they are contacted directly by the vendor for payment; in this situation, once aware of the past-due payment request, AP contacts the applicable department to obtain a PO. To help mitigate the risk of missed invoices, AP periodically accesses the ctcLink sub-modules utilized by the Purchasing department in 'read-only' mode, and reviews to see what POs are past 30 days outstanding.

College departments (including Purchasing) are disincentivized from intentionally withholding invoices or POs due to controls within the ctcLink system; AP staff are the only users which have system authorization to create vouchers and execute payments. Additional controls include segregation of duties over payments; the only staff which have access to print and mail physical checks are separate from the AP department; other non-AP staff are responsible for dispatching ACHs which were executed by AP to destination banks. A positive pay file for ACH transactions is also sent automatically to the recipient banks in a 'behind the scenes' process.



# State of Washington

## *Expense Classification*

Appropriate classification of expenditures begins at the departmental level. All budget and expense coding (i.e., chartstrings) for expenditures are classified according to OFM guidelines and its published charts of accounts (as contained in SAAM chapter 75). The Colleges specifically follow the State Board CLAM manual, which is designed to comply with these OFM guidelines. The CLAM manual provides guidance on how to set up chartstrings based on department (i.e., whether departmental activity is student-related, a proprietary function, etc.). Budget chartstrings are required before expenses can be paid; ctcLink will not allow processing of transactions to invalid budget chartstrings. Chartstrings tell the ctcLink system how to record accounting information such as fund, department, and class code; AFRS classification is specifically driven by ctcLink fund designation. A list of AFRS fund definitions and Colleger roll-up fund information can be found on OFM's website at: <https://ofm.wa.gov/accounting/fund-reference-manual/definitions-fund-types-and-roll-funds> and <https://ofm.wa.gov/accounting/fund/rollup>.

Specifically, the AFSRS Higher Education Special Revenue Fund primarily accounts for tuition, student fees, and grants/contracts received for educational and research purposes. As such, there are approximately 35 ctcLink funds at the College-level, which roll up to this AFRS Higher Ed fund. Common examples of these ctcLink roll-up funds include: 145 (grants and contracts account), 148 (dedicated local account), and 149 (operating fees account). For the majority of expenses, College departments only have one associated ctcLink roll-up fund which they are billing to. Departmental budget managers are required to review and approve all expenses during the PO creation process, ensuring that the correct chartstring (including fund) was utilized in the transaction. Finally, when creating and approving vouchers, AP staff reviews that chartstrings (including fund) agree to approved PO information (**Key Control 1 - Classification**). As an additional control, departmental budget managers review month-end budget reports, ensuring that all expenses are expected, and are hitting the correct accounts, funds, etc. If corrections are necessary, they submit a revenue/expense transfer request to AP, and AP staff then create a correction JV within the AP sub-module of ctcLink.

## *Expense Recognition*

Expenses are recognized at the time that a voucher is approved by AP staff, resulting in an automatic credit to the generic AP liability account (general ledger account 2000010), and a debit to the appropriate expense account. During the daily AP pay cycle, when an invoice is subsequently paid, ctcLink then automatically debits the AP liability and credits cash. A transaction can be identified using JV prefix, to determine whether it was initiated via voucher approval versus the pay cycle.

To mitigate the risk of improper expense recognition, the AP department pro actively communicates end-of-year deadlines and reporting requirements to all College departments annually, beginning as early as March. These notifications are sent out multiple times up through year-end. AP also hosts several trainings on year-end requirements for budget managers and supervisors. Additionally, AP maintains a year-end "accrual spreadsheet", requiring that AP staff carefully track all vouchers which are approved beginning on July 1st, through the first week of August (**Key Control 2 - Completeness**). The purpose of the spreadsheet is to ensure that staff are carefully considering which fiscal year is applicable for payments occurring near year-end. If a payment made after year-end is applicable to the prior period, AP staff have two options. Prior to a mid-July cutoff date, AP staff can simply change the voucher dates. After this cutoff date, they must manually accrue the expense via JV.

# State of Washington

## *General Ledger Reconciliation*

As discussed above, general ledger entries are recorded automatically by ctcLink during AP processes. On a monthly and year-end basis, the Finance team runs approximately 40 SMARTER queries, to identify errors in general ledger reporting, through comparison to ctcLink reporting. The review looks for incorrect combinations of chart fields, bad chartstrings, unusual accounting entries (such as expenses with a credit balance), etc.

## Payroll Disbursements

### *Expense Classification*

As discussed above for general disbursements, appropriate classification of payroll expenditures relies on accurate budget and expense coding (i.e., combo codes) at the College level. AFRS classification is specifically driven by ctcLink fund designation, and the College develops combo codes (including fund) in accordance with the State Board CLAM manual and OFM guidelines, ensuring accurate ctcLink fund roll-up to the AFRS Higher Education Special Revenue Fund. Combo codes for employee salary expense is set-up within the ctcLink Human Capital Management submodule (HCM) at the time a new employee is hired, and edits are made on a as-needed basis.

The College provided the following examples of how it classifies payroll combo codes:

- Fund 145 - grant-funded employees
- Fund 149 - classified and non-exempt State-funded employees
- Fund 148 - self support employees (e.g., class fees and continuing education, which helps fund certain positions)
- Fund 001 - exempt State-funded employees
- Fund 569\* - food service employees
- Fund 524\* - student & activity fee funded positions
- Fund 846 - financial aid employees
- Fund 850 - work study employees
- Fund 448\* - printing service employees
- Fund 570\* - athletics and radio employees
- Fund 573\* - housing employees

*\*All 400-series and 500-series fund coding represents Enterprise (proprietary-type) funds.*

The College allows only three individuals with adequate training and experience to create or edit payroll combo codes in accordance with OFM guidelines, ensuring accurate fund roll-up to AFRS (**Key Control 3 - Classification**). For hires which receive salary grant funding, combo codes are created by an individual in the Grants & Contracts department. For non-contracted (i.e., State funded) hires, an individual from the Budget department creates the relevant combo codes. All combo codes contain the following information: fund, class, department, purpose, and account. Grant-funded employee codes also contain project and activity information.

# State of Washington

## *Expense Recognition and General Ledger Reconciliation*

Approximately 5 days after the end of a pay period, a Journal Voucher (JV) auto-generates from HR HCM data, and is set to auto-post, backdating to the last day of the pay period (i.e., the year-end 6/30 JV posts approx. 7/5, but backdates to 6/30, so that it's recognized within the correct fiscal year and accounting period). This process was set up by the State Board on behalf of all community colleges within their oversight; the colleges are not supposed to edit the JV, other than extremely rare occasions where it may be so fundamentally wrong, that it wouldn't post to the General Ledger (GL). For minor errors or adjustments, the College would create a correcting JV and post it separately.

The auto-posted JV credits AP net pay liabilities and benefits, and credits offsetting expense accounts. When the liability is subsequently paid, the College is then responsible for reviewing their bank statement and manually posting the payroll liability reversal (includes crediting cash), dating the manual reversal JV with the same date as the paydate (the 10th and 25th of each month). After each pay period (including at year-end), Jennifer McMillan (Fiscal Reporting Manager) performs a GL reconciliation, prior to completing the manual payroll liability reversal (**Key Control 4 - Completeness**). During her reconciliation she manually pulls HCM data queries and ensures that data agrees to the bank statement and GL accrual.

## Identified Weaknesses

None.

## **STEP 2: Confirm Key Controls**

**Key Control 1 (Classification) - All vouchers are reviewed and approved by AP staff, ensuring that chartstrings (including fund) agree to applicable Purchase Orders.**

We identified voucher 00014859 to vendor Sysco Seattle Inc. from the expenditure detail (QFS\_AP\_VCHR\_PYMT\_WIP) provided by Jennifer McMillan (Fiscal reporting Manager). We then accessed ctcLink, and utilized the following path: Menu-->Accounts Payable-->Review Accounts Payable Info-->Vouchers-->Voucher. We searched for voucher 0014859, and reviewed the following from "voucher details": Vendor: Sysco, Voucher ID: 00014859, PO Number: 0000002731, Amount: \$1,949.24, Account: 5030130, Fund: 569, Dept: 14420, Class: 262, Desc: cans, food, and beverage package, Accounting Date: 4/30/2024, Approval History: Roselle Hay (AP Specialist Approver) on 4/30/24 at 4:38PM. We additionally reviewed the attached invoice, noting: Date: 4/24/2024, Vendor: Sysco, Amount: \$1,949.24, For: fresh vegetables. We then viewed 'Review Accounting Entries', noting that the entry was recorded as follows: Accounts: 5030130 and 2000010, Dept: 14420, Class: 262, Fund: 569, Journal Date: 4/30/2024. Next, we utilized the following ctcLink path: Menu-->Purchasing-->Purchase Orders-->Review PO Information-->Purchase Orders. On the "Purchase Order inquiry" screen, we searched for PO 0000002731, and reviewed the following from the "details" tab and "Distributions for Schedule 1" attachment: Req ID: 0000002709, Requester ID: 101040671, Requisition Name: Sysco Seattle, Attention To: Food Services, Allocation: 100%, Chartfields: Account 5030130, Fund 569, Dept 14420, Class 262. We conclude that chartstrings are consistent across the AP voucher, Purchase Order, and accounting entries. The AP voucher was appropriately reviewed and approved by Roselle Hay. **No issues noted.**

**Key Control 2 (Completeness) - All vouchers approved from July 1st through the first week of August are required to be tracked**

## State of Washington

**by AP staff on a year-end 'accrual spreadsheet', to ensure proper expense recognition in the appropriate reporting periods.**

We obtained a copy of an Excel workbook titled "FY24 YE AP Accruals" from Roselle Hay (Accounting Manager). The workbook contained 3 tabs titled 'AP vouchers FY24', 'Deadline Dates', and 'Accrual instructions'. The 'Accrual instructions' tab showed that an AP Accruals account was authorized by Loanne Wang as of 6/30/2022, and that Roselle Hay was authorized to approve entries to this account. The 'Deadline Dates' tab gave instructions to post AP vouchers with June accounting dates through the July 10th cut-off date for sub-module close. The instructions also stated that such vouchers must be added to the AP accrual spreadsheet. The tab also contained a screenshot of communications which were pushed through to various College departments, instructing how to report and obtain approval for invoices received by AP past year-end. The 'AP vouchers FY24' tab contained 195 vouchers, received by AP between 7/1/2024 and 8/8/2024, totaling \$1,823,621.16. For each voucher, AP staff indicated whether the expense was approved as a FY24 period 13 accrual. **No issues noted.**

**Key Control 3 (Classification) - The College allows only three individuals with adequate training and experience to create or edit payroll combo codes (on an as-needed basis) in accordance with OFM guidelines, ensuring accurate fund roll-up to AFRS.**

We reviewed the ctcLink user access listing for budget combo code changes (user role 'ZZ HR Combo Code') on 10/17/2024, noting that three College individuals were granted access as expected: Sharon Kussy (Budget Director), Sung Moon (Grants and Contract Manager), and Loanne Wang (Budget Analyst 4). We specifically note that, as expected, at least one individual is from the Budget Department, and one is from the Grants and Contracts Department. We additionally note that these individuals are highly experienced, long-standing College employees, who are familiar with State Board and OFM classification requirements. However, during our review, we additionally noted four individuals with unexpected user access: Kelly Paustain (previous Budget Director), Natalyia Matkivska (Admin Services Manager), Jenifer Cook (Bookstore Buyer), and Chika Risteen (Program Coordinator). Per follow-up inquiry with Jennifer McMillan (Fiscal Reporting Manager), we found that these four individuals likely should not have this user access role; however, they may have access due to their work at other colleges. Jennifer has submitted an internal ticket to see if user access for these individuals can be removed from Bellevue, without affecting their other work **(Control Weakness 1). See issue in conclusion above.**

**Key Control 4 (Completeness) - After each pay period (including at year-end), the Fiscal Reporting Manager performs a reconciliation between ctcLink HCM data, monthly bank statements, and GL accrual entries, ensuring that data between these systems is accurate and complete.**

We obtained a copy of 2024 year-end payroll reconciliation from Jennifer McMillan (Fiscal Reporting Manager) in an Excel workbook titled "FY2024 06B Payroll Recon - HCM to GL". On the "Summary" tab, we could see from summary pivot tables that FY24 salary expense per HCM as of 6/30/2024 was \$84,539,200, and that FY24 salary expense per the GL as of 6/30/2024 was also \$84,539,200. On the 'HCM' tab, we could see the full population of HCM data (source data for the HCM pivot table), which was obtained through query 'CTC\_HR\_ACCTG\_LINE\_PAY\_PERIOD'. On the 'GL - PAY' tab, we could see the full population of GL data (source data for the GL pivot table), which was obtained through query 'QFS\_GL\_ACCOUNT\_ANALYSIS'. Within the pivot tables, Jennifer performed an account by account comparison at the fund level for HCM vs GL data, in order to identify the source of any variances (no variances noted).

Next, we obtained a copy of the June 2024 year-end payroll liability reversal workbook from Jennifer, titled "Reverse Liab 06B". This workbook

## State of Washington

specifically reconciled the last pay period of FY24 (pay period ending 6/30/24). We note that the HCM query 'QHC\_PY\_CR7020' was utilized and filtered for the pay period end date of 6/30/2024, and additionally filtered to separately present employee benefit liabilities from employee net payroll liabilities. The auto-JV net pay liability for 6/30/24 totaled \$(2,299,466.99). Jennifer's workbook verified that this exact amount was debited from their bank account on 7/10/24. Her workbook additionally compared these amounts to GL data using query 'QFS\_GL\_ACCOUNT ANALYSIS' for account 2011015. All amounts agreed without exception. **No issues noted.**

### **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at '**MAX**'.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at '**MAX**' because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **J.4.PR.G - Community & Tech College Testing - Bellevue**

*Procedure Step:* Education Expenses - Testing

*Prepared By:* JLE, 10/9/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion:

Testing Strategy:

### **COMPLETENESS**

The following is a list of **considerations** for testing the completeness assertion for expenses/expenditures.

# State of Washington

Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

## **Detail Roll-Up**

Compare totals from general ledger to accounts payable, payroll or other subsidiary software modules.  
Review the government's reconciliation of general ledger to subsidiary systems.

*Detail roll-up testing is not sufficient audit evidence by itself since it only entails comparing different sets of the entity's own accounting records. However, it may be combined with other substantive tests to address identified risks.*

*For example, if substantive testing is performed at the subledger level, it may be combined with a test that the subledger detail accurately rolls up to the general ledger or financial statements.*

## **Cut off / Improper Expense Recognition**

Scan expenditures recorded 1-3 months before and/or after fiscal year end (expenditures not charged to the current period). Based on the scan, test selected or sampled expenditures to determine if the expense should have been reported in the current period.  
Inquire with AP clerks regarding invoices held, but not entered as of year-end (ie: due to pending litigation or disputes).

## **Unrecorded Expenses**

If the entity reconciles recorded revenues and expenses to bank activity, then reviewing monthly reconciliations and evaluating or testing reconciling items.

## **Accounts Payable**

If entity uses a warrant clearing account for vendor payments, review the entity's year-end reconciliation of recorded vendor payments with disbursements from the clearing account.  
Review edit check reports from the AP system that might indicate missing payments.

## **Payroll**

If entity uses a payroll clearing account, review the entity's year-end reconciliation of recorded payroll with disbursements from the payroll clearing account.

Perform an expected payroll test by taking the prior audited payroll amount and adjusting it for expected changes.

*The analysis should consider changes in employees, COLA increases, salary scale increases if automatic, changes wages or benefits due to changes in policy or union negotiations changes, etc. Sources for these expectations should be obtained apart from the payroll records that are being tested. Since the auditor would not expect to be able to precisely predict payroll, the auditor should document a reasonable range within which actual payroll is expected to vary from the auditor's prediction.*

If the board directly approves salaries for a significant amount of employees, verify whether the actual salaries for these employees is within an expected reasonable range of the approved salary.

# State of Washington

For small entities, compare payroll by employee to known employees per observation, organization charts or a phone list. Review edit check reports from the payroll system that might indicate missing payments.

## **Unrecorded Liabilities**

Evaluate liabilities directly related to expenses for completeness. See the completeness steps for current and non-current liabilities for testing considerations.

*For example, if the entity reports a self-insurance liability, the auditor might evaluate whether the change in the liability (and related expense) was determined and recorded. If no liability was reported, then the auditor might determine whether such a liability (and associated expense) should have been reported.*

**OPEB** - auditors should use the OPEB Testing Strategy workpaper available in the Store for auditing OPEB expenses.

**Pollution Remediation** - auditors should use the Pollution Liability Testing Strategy workpaper available in the Store for auditing pollution remediation expenses.

## **Removing Expenses from Accounting Records**

Search for manual journal entries that credit (decrease) expenditures. Consider testing selected transactions.

Identify transactions that void, cancel, or manually adjust transactions in subsidiary AP or payroll systems. Auditors may conclude that the total amount of such transactions are trivial or otherwise reasonably small. Or auditors may sample or select transactions for testing.

*Also see considerations under the "Not recording expenses" section.*

## **Interfund Expenses**

For internal service fund charges, see testing strategies for internal service funds in the Accountability folder. For other types of internal charges, see testing strategies for Internal Activities.

## **CLASSIFICATION**

The following is a list of **considerations** for testing the classification assertion for expenses/expenditures.

Results from planning procedures (inherent and control risk assessments) are the basis for the auditor's design of substantive tests.

Sample transactions for correct classification. *Use the "Sampling for FS Substantive Testing" spreadsheet available in the Store to calculate sample size and make any projection of likely misstatement to the population.*

If planning has identified a limited population that is high risk (ex: certain transaction types and/or line items within an opinion unit), scan these populations and test selected transactions.

# State of Washington

## Journal Vouchers

Search for manual journal entries that reclassify expenses/expenditures from one opinion unit to another without recording a balance sheet transaction, other than a direct charge to fund balance (debit and credit to expenditure and fund balance for each opinion unit, respectively). Test selected journal entries based on risk.

Search for manual journal entries that reclassify expenses/expenditures from one line item to another. Test selected journal entries based on risk.

## Vendor Payments

Review the top vendors paid by opinion unit or line item (preferably as a multi-year trend) and evaluate whether the vendor meets expectations in relation to the activities of the fund. Test transactions for each unexpected vendor based on risk.

Test selected or sampled transactions for correct classification.

*NOTE: this test may be combined with expenditure tests for other attributes. For example, expenditure testing for accountability or single audit purposes may also be used for classification testing.*

## Payroll

Scan totals charged to each opinion unit by employee (preferably as a multi-year trend) and evaluate whether the allocation of employee's time to that opinion unit meets expectations based on job titles, organization charts, observation or the phone list. Follow up on unexpected allocations by review of timesheets or employee interviews.

Perform an expected payroll test by opinion unit.

Test a sample of pay periods for salaried and hourly employees to ensure that expenditures are being classified to the correct opinion unit. This test should verify both the correct allocation of direct charges and that leave and benefit costs are allocated in the same proportion as direct charges.

## Cost Allocation Plans / Internal Service Fund Allocations

Review cost allocation plans or internal service fund charges to confirm that the classification of joint costs to different opinion units is supported.

*See example testing strategies for these areas located in the Accountability cabinet .*

Guidance/Criteria.:
---------------------

Record of Work Done.:
-----------------------

## Significant Balances and Assertions

Governmental Activities- Education- Higher Education Expenses - Completeness, Classification



# State of Washington

## Higher Education Special Revenue- Charges for Expenses - Completeness, Classification

Controls are documented in the "Education Expenses - Controls" step, see: [[Education Expenses - Controls](#)]. See testing at: [[Education Expense Testing](#)].

### **Substantive tests performed to meet the Completeness assertion**

We performed an analysis of the expense balance composition for Bellevue, utilizing SAO DARS queries to examine makeup by AFRS object coding, determining we would focus testing on objects A (payroll) and E (accounts payable).

Payroll - we considered completeness of the entire year's payroll expense by performing a detailed roll-up from ctcLink's Human Capital Management (HCM) submodule to the College's general ledger, comparing an HCM gross payroll expense detail (provided by Jennifer McMillan, Fiscal Reporting Manager) to ctcLink query 'QFS\_GL\_SRECNP\_DETAIL' (obtained directly by auditor). We found a \$26,165 variance between these two reports, which is beneath the floor of materiality. We tested for completeness at year-end (i.e., expense recognition) by filtering the HCM gross payroll expense detail for the 7/10/24 paydate, which relates to the last pay period of the fiscal year (6/15 - 6/30). As this report provides gross pay detail, we additionally filtered to remove tax and benefit deductions, arriving at a year-end net pay liability amount. We then compared this amount to payroll liability per the general ledger (account 2011015) using query 'QFS\_GL\_ACCOUNT ANALYSIS' (obtained directly by auditor). We found a \$14,120 variance, which is beneath the floor. Finally, we traced the year-end payroll liability amount to the U.S. Bank statement for July, considering whether the 7/10 payment matched recorded liability amounts. We found that the payment matched recorded liability amounts without exception. **No issues noted.**

Accounts Payable - we obtained a detailed voucher listing of AP vouchers paid to vendors during Qtr 1 of FY25. Using the sampling spreadsheet from the TeamStore, we randomly sampled 21 testing selections, plus 3 individually significant selections, for a total of 24 testing selections. For each selection, we examined vendor invoices, general ledger data (from FY24 and FY25), and a year-end accrual detail, to determine whether the expense was recognized in FY24 or FY25. We found 6 exceptions totaling \$8,757 where the expense was recognized in an improper accounting period. This misstatement projected to \$966,838, which is beneath the floor. **No issues noted.**

### **Substantive tests performed to meet the Classification assertion**

We performed an analysis of the expense balance composition for Bellevue, utilizing SAO DARS queries to examine makeup by AFRS object coding, determining we would focus testing on objects A (payroll) and E (accounts payable).

Payroll - using the sampling spreadsheet from the TeamStore, we randomly sampled 21 testing selections from FY24 payroll expenditures recorded within Higher Education Special Revenue Fund roll-up funds. For each selection, we obtained Personnel Action Forms or HR contracts from Olga Krichevskaya (Payroll Director). We examined each employee's position description and department,

## State of Washington

determining whether the associated payroll for these employees appropriately represents education-type expenses per the OFM fund definition. **No issues noted.**

Accounts Payable - using the sampling spreadsheet from the TeamStore, we randomly sampled 21 testing selections from AP vouchers paid to vendors during FY24 which were recorded within Higher Education Special Revenue Fund roll-up funds. For each selection, we examined vendor invoices, determining whether the associated expense appropriately represents education-type expenses per the OFM fund definition. **No issues noted.**

### J.4.PRG - Community & Tech College Testing - Bellevue

*Procedure Step:* Federal Grants in-Aid - Controls

*Prepared By:* SRC, 10/24/2024

*Reviewed By:* CJG, 11/1/2024

Purpose/Conclusion:

**Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

**Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted no material weaknesses or significant deficiencies in internal controls.

Testing Strategy:

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

# State of Washington

## **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

## **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

# State of Washington

## **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

## **STEP 4: Control Testing**

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year*

## State of Washington

*audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

Record of Work Done:

### **Significant Balances and Assertions:**

Internal controls in the Community and Technical College System address the following balances:

Governmental Activities - Education - Higher Education Operating Grants and Contributions - Occurrence  
Higher Education Special Revenue - Federal Grants-In-Aid - Occurrence

See lead sheet here: [[Lead Sheet](#)]

## **1. Gain an Understanding of Internal Controls**

# State of Washington

On September 19, 2024, we met with Jennifer McMillan, Finance Manager, and Sung Moon, Grant and Contract Compliance Manager, to gain an understanding of internal controls over Grant revenue and expense as it relates to significant balances reported to AFRS by SBCTC on behalf of the College. We identified that we would be focusing on Department of Education (DOE) revenue, including Title III, Trio, and Pell Grants, which make up 91% of federal grants in aid.

## **Department of Education-Title III, TRIO, and Pell Grants**

### **Pell Grant**

Students can apply for Federal Pell grants using the free application for federal student aid (FAFSA), and they are awarded aid based on their need and responses to the questions on the form. The student award information is sent to the financial aid (FA) department at the college where FA staff award students in the ctclink system so it can be applied to tuition & fees. Amounts in excess of this can be refunded to the student.

When tuition is due, the student financials (SF) staff run a "group post" to post the Pell award amounts to student accounts. FA Disbursements occur every Thursday - beginning the Thursday before the Quarter starts (only applies for the FAFSA year of application). The FA Disbursement pays off the student's eligible charges - what is left over of the FA is now a credit on the student's account. The financial Aid department reconciles the Federal Pell grant awards as applied to student accounts to ensure that all eligible student awards paid out or refunded properly.

### **TRIO and Title III**

The TRIO Grant is awarded to the College by the DOE to help fund Student Support Services. TRIO is a program that provides individualized support services to students with limited income, first-generation college students, and students with disabilities to assist them with their academic success. To apply for TRIO, students meet with TRIO Staff and fill out an application electronically. Once approved, the Student goes through an intake process and is then able to make appointments with an Advisor to receive assistance services in a number of areas, such as Financial Literacy and Academic Advising.

A Title III Grant in the amount of \$2,094,323 was awarded to Bellevue College in October 2019, to be distributed over a five year period (2019-2024). The grant has been used to improve retention, completion and transfer rates of all students while also closing achievement gaps experienced by underserved populations. The College has used the grant to fund numerous projects, including Lead Peer Educators, BC Pathways, and First-Year Seminar.

TRIO and Title III grants are both Cost Collect grants, which means that the College is reimbursed for Grant related expenses via draw-downs, up to the award amount. On a monthly basis, Sung runs a query in ctclink to generate a report of grant related expenditures, she then generates a grants interface for the duration of the draw, which only pulls billable expenses, and compares the reports to ensure the numbers tie out. For cost collect grants, ctclink automatically generates an invoice when Sung pushes a button to confirm that the numbers are balanced. She then logs

## State of Washington

into the DOE Portal to initiate a draw for the funds. The revenue is then recorded in a special CAPC account until the funds have processed, after which the CAPC is cleared out and the revenue is credited to a regular AR.

### **Washington College Grants**

The Fiscal Analyst 5 (FA5) (vacant) compares the expense data from ctcLink with the award data from the WSAC website, to ensure the amounts match, prior to making a draw-down from WSAC. After the draw-down has occurred, the FA5 creates billing (new: requests billing to Billing dept) for actual revenue drawn and submits for approval. Within a week after funds are requested, WSAC sends an email confirmation to Jennifer McMillan and the FA5, notifying them the money has been wired directly to the College's bank. The FA5 then forwards this email to relevant Accounting staff for processing with appropriate Billing info. A Fiscal Analyst posts the revenue receipted in the ctcLink system.

The Washington College Grant funds are drawn for each student individually. Jennifer explained that they reconcile student accounts with WSAC and Federal Aid on daily basis because WSAC draws must match the student's account balance exactly, and the data often does not match in all of the systems due to timing and account activity.

### **Running Start & CEO Programs (Not Updated for 2024)**

Roselle Hay, Accounting Manager, and Agnieszka Skoczylas, Travel Coordinator/Student Accounts, handle the billing and receipting of the Running Start & Continuing Education Opportunity (CEO) program revenues. Invoices for the Running Start & CEO programs are generated in the High School Programs (HSP) office and are sent out to the school districts participating in the Running Start and/or CEO programs. A copy of the invoice is emailed to Agnieszka; she prints out each of the districts quarterly (Fall, Winter and Spring) Running Start and/or CEO program invoices and sets up a receivable for each school district in the ctcLink system. An A/R code is generated and Agnieszka writes the code on the corresponding invoice. If an invoice has been corrected, the HSP office will provide Agnieszka with an updated copy of the invoice and she will make the update to the system to reflect the new invoice amount.

The school districts send running start payments via a physical check, which includes the program name, invoice amount, and the school's quarter term. When the checks arrive in the Finance office, a "**Daily Check Log**" is passed around for staff to initial the receipt of the (two) check copies. Agnieszka writes the A/R code (RS-abbreviated school district) on both copies; she retains one copy and attaches it to the corresponding invoice. She passes the other copy on to Vicky Kazachenko, Fiscal Analyst, who posts the payment into the ctcLink system under the customer account previously set up by Agnieszka.

If there is an outstanding payment, Agnieszka emails the HSP office on a monthly basis and includes the Director and Program Specialist. A list of outstanding invoices is provided to HSP to follow up with the school districts requesting payment for past due. On a quarterly basis, Roselle Hay, Accounting Manager, reviews the accounts receivable subledger to ensure the Running Start and/or CEO payments are current. Roselle's subledger takes in data from all third-party payees; she can see the customer, the amount paid for the "year-qtr", and whether the invoice has been paid. She pulls in current data from the PeopleSoft system into her receivable subledger to scan for any outstanding payments, including

## State of Washington

Running Start and/or CEO. From her knowledge of the coding for year-qtr, Roselle can identify whether an invoice has been paid out and if there are any outstanding payments. Roselle checks in with Agnieszka on invoices outstanding for more than 90 days.

### **Local Grants & Contracts (Not updated for 2024)**

The College has a local grant committee that reviews potential grants submitted by the College's various departments. After the grant has been applied for and approved, Sung sets up the grant in the system with the budgeted amount. She reviews the proposal, award letter, the amount of award, and the contract to ensure the information in the system is input correctly.

On a monthly basis, Sung performs a reconciliation for each grant and sends an email notification to the department that received the grant indicating if the funds are not being used or if they are over spending. She will meet with departments as needed to discuss the grant, funding, and/or review the remaining balance. The department responsible for the grant creates the invoice for reimbursement and submits it to the grantor. Sung is responsible for creating some of the grant invoices. Sung receives a copy of the invoice from the department and enters the invoice into the College's receivables system. She then enters the grantor's information and invoice amount into her "Grant Accounts Receivables" tracking spreadsheet. To ensure she has received all related grant invoices, she utilizes the OBIS website on a monthly basis and reconciles to her tracking spreadsheet. As the funds are received (either EFT or physical check) they are included in the Financial Daily check/bank log that goes around the finance office each day.

Sung receives two copies of the checks (or print out of EFT received), and notes the receivable information on each copy. She retains one for her grant folder, and passes along the second copy to Vicky Kazachenko, Accounts Receivable Accountant, to enter as a receivable in the system. Sung makes a note on the Grant Accounts Receivable spreadsheet with the check number, or the EFT date. At the end of each month, Sung uses a grant report to show all grants to reconcile the grant money received against what was budgeted.

The local contracts specify when payments are to be made to the College (monthly, quarterly, etc). Sung noted some of the payments related to local contracts have invoices, and some do not as the payment is based on the agreement. For local contracts with invoices, the same process as described above is followed. Payments related to local contracts without invoices are received at the College and entered into PeopleSoft by Vicky Kazachenko, Accounts Receivable Accountant.

### **Posting to the GL**

Financial aid is posted to the GL via a "second journal set" which posts the financial aid item types to the correct expense accounts to ensure the expense and revenue match up in the general ledger. Every Monday, SBCTC will run the process for the 2nd Journal Set (Monday – Sunday) - as an excel file Summary to the item type, put on or coming off the student's account (only activity during that time frame is captured). This makes it easier to do weekly reconciliations of the revenue and expense posted by FA item types. The Finance team will post this second Journal Set to the General Ledger on the same day (Monday) so that FA team is able to see GL expenses and post them properly using an offset with the internal cash account.



# State of Washington

Draw downs of federal grant funds from the Department of Education (DOE): The Grant and Contract Compliance Manager takes total grants expenses posted for the time period, less total revenue posted to ascertain the amount to be drawn down. This ensures they only draw down the revenue related the period. They then receive the funds through an EFT to the bank. They post the DOE revenue to the same chartstring or budget account code (department, fund, and class) as the expenses are reported to ensure that the amounts remain equal and balanced (**Key Control 1 - Occurrence**).

## **Summary of Key Control(s):**

**Key Control #1: The Grant and Contract Compliance Manager takes total grants expenses posted for the time period, less total revenue posted to ascertain the amount to be drawn down. This ensures they only draw down the revenue related the period. DOE Revenue ties to the same chart string or budget account code (department, fund, and class) as the expenses are reported to ensure that the amounts remain equal and balanced for the period (Occurrence).**

## **Noted Weaknesses are as follows:**

None.

## **2. Confirm Understanding**

**Key Control #1: The Grant and Contract Compliance Manager takes total grants expenses posted for the time period, less total revenue posted to ascertain the amount to be drawn down. This ensures they only draw down the revenue related the period. DOE Revenue ties to the same chart string or budget account code (department, fund, and class) as the expenses are reported to ensure that the amounts remain equal and balanced for the period (Occurrence).**

We reviewed the support for the Draw down and corresponding ACH deposit to the Bellevue bank account ending in \*2980 that occurred on 4/25/2024 in the amount of \$341,550.51. The recipient reference was PELL 23-24 for award No. P063P232396, which was authorized in an amount up to \$5,757,931.60 and had a remaining balance of \$1,396,482.51 at the time of the draw. The workbook also included a pivot table totaling the Pell item type expenditures by term (\$341,550.51) along with expenditures by term for the Supplemental Education Opportunity Grant (\$6,300), Subsidized Direct Loans (\$78,832), Unsubsidized Direct Loans (\$124,272), and Parent PLUS Loans (\$1,794), and a screenshot of a Federal Work Study salary draw (\$12,325.22) that was included in the total draw. We identified that these amounts combined were equal to the total Draw Request of \$565,073.73 submitted to the DOE. We also noted the deposit of the draw on the College's US Bank statement dated 4/26/2024. *No issues noted.*

## **STEP 3: Preliminary Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or

## State of Washington

material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

### **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

### **STEP 5: Final Control Risk Assessment**

**MAX** - We noted no matters involving internal control over financial reporting and its operation that we consider to be significant deficiencies or material weaknesses. However, we have assessed control risk at max because we have determined that substantive procedures alone will be effective to reduce detection risk to an acceptable level.

#### **K.1.PRG - Rely on Work of Other Auditors**

*Procedure Step:* External Auditor performs PART of audit

*Prepared By:* RKM, 12/10/2024

*Reviewed By:* SHW, 12/16/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

#### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for the University of Washington (UW), State Investment Board (SIB), Department of Retirement Systems (DRS), Local Government Investment Pool (LGIP), Fred Hutchinson Cancer Center, Washington Health Benefit Exchange, Valley Medical Center and Washington State Housing Finance Commission.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted **no** concerns with the work of other auditors to bring to the attention of management at the exit conference.

# State of Washington

## Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

### **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

## State of Washington

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be reviewed and incorporated into our audit as described in step 9 below.

**ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material

## State of Washington

Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

## State of Washington

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

Component auditor has performed the audit in accordance with GAAS or GAGAS.

Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:

Record of Work Done:

**Step 1** - We determined the significance of components audited by external auditors to the applicable opinion unit at [\[Final Planning Significant Balance Spreadsheet\]](#) and [\[External CPA Audit Significance\]](#).

**Step 2** - We considered attending key meetings between the external auditor and the government. We elected not to attend the exit meetings for the CPA audits.

**Steps 3 through 6 and 8 through 11** - See summary at [\[Work of Other Auditors - Summary\]](#).

**Step 4** - See audit plan at [\[ACFR Audit Plan\]](#).

### K.1.PRG - Rely on Work of Other Auditors

*Procedure Step:* Percent of Work Performed by Other Auditors

*Prepared By:* SHW, 12/12/2024

*Reviewed By:* RKM, 12/12/2024

## State of Washington

Purpose/Conclusion.:

**Purpose / Conclusion:**

Determine the percentage of total assets and revenues/additions audited by other auditors by opinion unit for our report.

**Source:**

OFM draft Financial Statements (12/6/24)

Access queries run on ACFR File (12/6/24)

Testing Strategy.:

Auditors are **required** to calculate percentages of total assets, net assets, and revenues covered by other auditors on whom we are relying in order to properly reference their work in our report. Auditors should use final financial statement figures for these calculations and only include the work of other auditors deemed material in the calculation

Guidance/Criteria.:

Record of Work Done.:

We preformed this analysis at: [Percent Audited by Others FY24].

For purposes of our financial statement opinions, we calculated the percentage of assets, net position and revenues/additions audited by others on whom we are placing reliance.

The first tab on the spreadsheet above contains total state assets, net assets/fund balance, and revenues/additions by opinion unit taken from the basic financial statements. The first tab also contains the associated amounts audited by others on whom we are placing reliance, by opinion unit. Total assets, net assets/fund balance, and revenues/additions audited by others are divided by the state totals to obtain the percentages to be placed in the audit report. The remaining tabs show the detail balances by agencies and associated ACFR Access queries that were used to obtain the information from the ACFR file. The final tab shows the table to be used for the F-Report.

**K.2.PRG - Work of Other Auditors - UW**

*Procedure Step:* Controls - UW Workday GL to AFRS

# State of Washington

*Prepared By:* BM2, 11/22/2024

*Reviewed By:* SHW, 12/10/2024

## Purpose/Conclusion.

### **Purpose:**

To gain an understanding of internal controls and assess control risk in order to help plan the nature, timing and extent of substantive testing.

### **Conclusion:**

We have gained an understanding of internal controls and assessed control risk at **maximum**. Therefore, we **will not** place reliance on controls. Our understanding of internal controls and control risk assessment will be used to help plan the nature, timing and extent of substantive testing.

We noted the following material weakness in internal controls:

During FY24, UW financial reporting did not complete fund level reconciliations to adequately support balances reported in the ACFR. UW does not verify that all financial statement balances are translated appropriately for state reporting. OFM did not perform sufficient procedures to verify UW balances in AFRS were accurate. See issue [F: UW consolidation, reconciliation and adjustment of balances].

## Testing Strategy.

The following procedures are **required** for all relevant systems:

*Optional:* List the financial statement balances and relevant assertions addressed by the understanding.

### **STEP 1: Understanding of Controls**

Gain an understanding of the internal control process, identify key controls over relevant assertion(s), and note any control weaknesses.

*The auditor's understanding should include:*

*Business processes relevant to financial reporting of the relevant assertion for the material balance. Processes should encompass automated and manual procedures by which transactions or events are identified or initiated, authorized as needed, recorded, processed and corrected as needed.*

*Original accounting records and how records are rolled-up to intermediary ledgers and transferred to the general ledger or financial statements.*

*Detailed descriptions of key controls. Effective key controls provide reasonable assurance that material misstatements in relevant assertions will be prevented or detected and corrected timely. If there is not a key control designed to address a relevant assertion, a*



## State of Washington

*significant deficiency likely exists. Depending on the magnitude and likelihood of potential effects and any compensating controls, the deficiency may represent a material weakness.*

*In gaining an understanding of controls, consider the overall understanding of Entity-Level control elements as documented in the "Entity-Level Controls" step as they relate to this particular system.*

### **STEP 2: Confirm Key Controls**

Confirm your understanding to determine whether key controls have been placed in operation (*whether the entity has actually implemented key controls*).

*A walkthrough of a transaction is considered the most effective way of corroborating your understanding of internal controls. Inquiries, inspection of records and observation are other acceptable methods. However, inquiry alone is not sufficient to determine a control has been implemented. For key controls confirmed, indicate any documents (include title of document used by the government), journals ledgers, reports, or other information you examined during the confirmation process, including automated reports or documentation. Describe the manual and automated processing that you observed or performed and responses to your inquiries.*

*Indicate the name and position of the employee who performed the procedure. Consider the competence and understanding of the person performing the control.*

*When a key control is discovered to not actually be placed in operation, a significant deficiency or material weakness likely exists.*

*If a key control is automated, the confirmation of our understanding should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

### **STEP 3: Preliminary Control Risk**

Evaluate the results and document a preliminary control risk assessment. Consider whether internal control weaknesses identified represent material weaknesses or significant deficiencies.

*Control risk is the risk that material misstatements would not be prevented or detected timely by internal controls. In order to support a control risk assessment that is less than MAX, the auditor must test the operating effectiveness of controls in step 4A. Regardless of this decision, the auditor must report any significant deficiencies or material weaknesses discovered in either the design or operation of controls. All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.*

### **STEP 4: Control Testing**

## State of Washington

If the auditor plans to support a control risk assessment of less than MAX, test the operating effectiveness of key controls (*whether controls were consistently and effectively applied*).

*If a key control is not consistently or effectively applied, a significant deficiency or material weakness likely exists. If exceptions are noted, auditors should follow up to understand why the exception occurred and the potential consequences. Additional testing or changes to the audit plan may be needed, based on auditor evaluation and follow up of exceptions.*

*If a key control is automated, the auditor must also test related general controls. General control testing should be documented in the appropriate "IT Control Testing" step pulled down from the SAOStore and be hyperlinked with this step. Auditors should consider contacting Team IT Audit for assistance.*

*An optional IC Cycling Matrix is available in the SAOStore to document the history of key control testing for material systems. Evidence about the operating effectiveness of controls obtained in prior audits may be used so long as the auditor documents a conclusion that it would be appropriate to rely on prior audit work, based on review of prior control testing and evaluation of Entity-Level control elements. In doing so, all of the following specific determinations must be documented:*

- A. Controls have not changed significantly since they were last tested. In making this judgment, auditors should consider whether any key controls or key staff who apply key controls have changed. Auditors should also consider whether the process surrounding the key controls has changed significantly, including policies, IT systems, processing steps, data sources, etc.*
- B. Controls are not related to a "significant risk" identified in the audit plan.*
- C. Controls are tested in the current audit for at least one other system, so that we are not relying on prior audit work for all control testing.*
- D. The prior work is from an audit performed within the last two cycles in an annual audit; or within the last cycle for a two or three-year audit. For example, on an annual audit if controls were tested for the period ending 2022, this work could potentially be relied upon for both the periods ending 2023 and 2024.*

### **STEP 5: Final Control Risk**

Evaluate the results and document a final control risk assessment. Consider whether any internal control issues identified represent material weaknesses or significant deficiencies.

*A material weakness exists when the design or operation of controls results in a "reasonable possibility" that controls will not prevent or detect material misstatements. A significant deficiency is a control deficiency that is less severe than a material weakness, yet important enough to merit the attention of the governing body. See the Policy/Standards tab for more guidance on evaluating whether an identified issue represents a material weakness or significant deficiency. **All potential material weaknesses and significant deficiencies should be discussed with the AIC or AAM, since they must be reported as findings.***

# State of Washington

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [2310](#) - Reporting Identified Audit Issues**

**SAO Audit Policy [6230](#) – Understanding Internal Control and Assessing Control Risk**

**[Financial Statement Audits](#) Planning Guide**

## **AUDIT CRITERIA**

Key criteria that auditors will likely use when testing this area.

**BARS [3.3.9](#) Capital Asset Management System Requirements**

**BARS [3.3.11](#) Controls Over Capital Assets**

Record of Work Done:

## **Significant Balance(s) and Assertion(s)**

Risks identified during brainstorm:

Although the Universities financial statements are audited by a CPA firm, there is a risk that the adjustments made to AFRS for state reporting may be incomplete, inappropriate or inaccurate, potentially affecting assertions in the higher special revenue, higher student services and higher endowment opinion units. In addition the UW implemented a new ERP (Workday) in FY24 potentially increasing risk.

There is a risk that the data converted from Workday to AFRS is not accurate and complete.

## **STEP 1: Gain an Understanding of Internal Controls**

We met with Anna Quichocho, OFM Financial Reporting Manager, on September 4, 2024 to gain an understanding of controls related to importing UW Workday GL data to AFRS.

We met with Susan Stolle, Associate Controller, Tina Young, Senior Financial Reporting Analyst, and Erick Winger, Controller, on September 17, 2024 to discuss controls related to data integration and reconciliation from WD to AFRS.

# State of Washington

## Background

University of Washington's financial statements are audited by external auditors. Our office evaluates the work done by external auditors and determines if we can rely on the audit reports issued by external auditors for significant components. **See the External Auditor performs PART of the audit step** [[External Auditor performs PART of audit](#)]. We perform additional procedures to ensure that audited balances from UW's financial statements are properly adjusted and transferred into AFRS for state reporting.

The Financial Accounting System (FAS) was University of Washington's primary financial accounting system and was implemented in 1974. In fiscal year 2024 (starting July 1, 2023) Workday Finance (WD) has replaced FAS as UW's primary financial accounting system. UW's financial systems are comprised of a variety of separate systems that have been integrated.

Closing UW's books at year-end requires data to be manually captured, analyzed, and adjusted for reporting in the State's legacy system. Anna Quichocho is the main contact for UW to assist in importing data from UW's system to AFRS.

## Workday Interface with AFRS

Monthly and at year-end, UW accounting and financial management staff oversee the electronic transmission of accounting data and transmit it to align with the State's legacy system. University of Washington prepares a crosswalk document at the end of each month to map workday coding appropriately to AFRS. There are 4 separate mapping documents (this includes one for spend category, ledger, revenue, and fund). See all 4 mapping documents as of 8/12/2024 at [[UW Workday to AFRS Mapping Documents](#)]. Eric Darst, UW Business Intelligence Engineer, runs a "Summary of Journal Lines" report from Workday Finance at the end of each month that includes raw data of all financial activity to be recorded. The data is provided via a text file through OFM's Secure file transfer site, MFT. The file uses the required AFRS 950 layout to ensure the data is integrated accurately and completely. Qing Gao, OFM IT Architecture Specialist, will export the summary of journal lines report from the MFT site and use the mapping documents to crosswalk Workday coding to AFRS coding. He uses SQL queries to append the raw data with additional AFRS coding from the mapping documents to allow the file to import properly with AFRS. Anna Quichocho, OFM Statewide Accountant, will scan the summary of journal lines report with AFRS coding to determine if there are any obvious systematic errors from the SQL query that will not allow the file to process in AFRS. Once Anna has reviewed, the import file is first processed through AFRS QE, a testing environment, to identify processing errors before posting to the production environment. AFRS QE will automatically generate an error report which will display an error code on each line that could not be processed (**Key Control 1**). OFM maintains an [error code manual](#) that explains each error code along with a suggestion to correct the error. OFM will provide the list of errors to UW to make corrections. OFM will process everything else from the import file that could be posted. Generally, a month's worth of transactions is about 2,000 lines and OFM will regularly see about 90 transactions that have errors and do not post. Tina Young, Senior Financial Reporting Analyst, will make corrections for error codes, as practicable.

The portion attributable to the discretely presented component units (Valley Medical Center and Fred Hutchinson Cancer Center) are sent to OFM, who includes the information in the State ACFR as a Major Component Unit. This portion is not recorded in AFRS, instead UW provides financial statements and an assigned statewide accountant inputs balances directly to the component unit financial statement. See financial statement

## State of Washington

controls for preparation of component unit financial statements at [\[Financial Statement Preparation\]](#) and [\[Understanding Methodology\]](#). Any blended components maintained by UW are included in their financial data that is imported to AFRS on a monthly basis.

We inquired with Anna Quichocho about differences between the new process for Workday interfaces and how FAS interfaced with AFRS. Per Anna:

- FAS would only import summary level data, Workday Finance allows for the reports to be transaction level

- Monthly import files include balance sheet and income statement activity. FAS import files only included income statement data throughout the year and balance sheet data was imported at year end.

- Monthly close is more timely. Files are typically fully integrated to AFRS 2 days before AFRS closes.

### Monthly Reconciliations

Susan explained the normal process for reconciling at month end includes preparing a reconciliation at the fund level from Workday (previously FAS) to AFRS. This reconciliation ensures that all amounts posted to AFRS are supported by Workday GL detail with any adjustments and reconciling items. With Workday's ability to import revenue/expense data at a detail level, UW no longer has to prepare an additional revenue and expense reconciliation. Revenue and expense accounts are included in fund level reconciliations. During FY24, these fund reconciliations were not in place. Susan stated that mapping workday GL to AFRS GL took a majority of the time this year and resulted in obvious errors that had to be corrected. In April 2024, UW began their fund level reconciliation process, however, there is no documentation that all fund reconciliations were completed at this time.

To prepare fund level reconciliations, UW Financial Reporting obtains trial balance detail from AFRS to Workday GL amounts. The reconciliation spreadsheets for each fund are used to reflect the audit trail from WD balances to final AFRS balances. The first step is to record a journal voucher in AFRS to "true up" all balance sheet activity in AFRS based on WD ending balances. The journal entries are converted through an mapping documents to establish AFRS coding, see [\[UW Workday to AFRS Mapping Documents\]](#). Reconciling items are entered into AFRS using a journal voucher to adjust the balances to the trial balances, and MJV's which are used to do adjustments strictly related to the presentation for UW's financial statements. UW financial reporting identifies reconciling items in fund level reconciliations provides them to OFM. Staff in UW's Financial Reporting unit prepare the fund level reconciliations for each fund and the controller reviews **(Key Control 2)**. The reconciliation uses Workday balance sheet and income statement GL in detail by GL account and then summarizes in total for each OFM GL account. OFM GL data is obtained via running an AFRS trial balance. Differences were categorized by reconciling item (potential errors or posted to category that UW doesn't agree with) or exceptions (items reviewed by UW that are not reconciling items but UW is comfortable with the difference). Exceptions can include things like timing variances or differences in detail of presentation from UW statements and ACFR.

UW financial reporting could not provide completed fund level reconciliations to OFM or SAO for 47 reported funds until November 2024. The resulting variances and reconciling items could not be adjusted by OFM like the standard process from prior years. **See control weakness reported here** [\[F: UW consolidation, reconciliation and adjustment of balances\]](#) **and in the conclusion.**

## State of Washington

At the request of SAO, UW also performs reconciliation of UW financial statement balances to identified significant ACFR balances in what is called a "natural class reconciliation." UW financial reporting will run AFRS queries and use internal balance sheet/income statement templates to compare GL amounts between AFRS and Workday (**Key Control 3**). We use the natural class reconciliations to assist in our testing procedures to trace UW financial statement balances to the ACFR. Although UW prepares reconciliations at SAO's request, UW does not verify that all financial statement balances are translated appropriately for state reporting. **We will include this in the weakness reported [F: UW consolidation, reconciliation and adjustment of balances].**

### Adjustments (Post Close Entries)

Adjusting JV entries (post close entries) are required to reconcile the differences between WD and AFRS for various reasons. The most common reasons for these JV entries are as follows:

- Certain account balances are recorded in one GL account in WD but need to be allocated to each fund for AFRS (e.g., Internal Lending Program (ILP) debt and payments, Vacation accruals, etc.)

- WD has a hard closing date of July 31 each year where AFRS is open through September 15th. Some transactions are adjusted in AFRS after July 31 for the fiscal year that ended, but not recorded in WD until the next fiscal year (e.g. Assets, depreciation expense, etc.).

- WD reports accounts as total balance, however AFRS requires certain account balances to show current and noncurrent portions.

- Reclassification JV entries are needed in order to break out the current and noncurrent portions of an account balance in AFRS (e.g. liability payments, debt payments, etc.).

- Total number of journal entries made to complete the adjustments and reconciliations may exceed 100 annually. Per Susan, she expects this to be higher for FY24 due to system conversion.

UW performs a series of post close entries to ensure that the balances in AFRS agree to the balances reported from the financial statements of the University. UW will create post close entries to adjust amounts, respond to error codes, and ensure accuracy of data from WD to AFRS. Post close entries are batched and integrated into AFRS in the same process as monthly data integration files (**Key Control 1**). For FY24, UW financial reporting processed 4 batches of post close entries.

### Key Controls:

**Key Control 1 - UW financial reporting imports Workday financial data to AFRS on a monthly basis using text files. AFRS automatically generates error reports to identify any financial data lines that would not appropriately post. UW financial reporting will review and correct error codes to ensure data from workday is accurately uploaded.**

**Key Control 2 - UW financial reporting identifies reconciling items in fund level reconciliations provides them to OFM. Staff in UW's Financial Reporting unit prepare the fund level reconciliations for each fund and the controller reviews**

**Key Control 3 - UW financial reporting performs reconciliations of UW financial statement balances to significant ACFR balances (at request of SAO).**

### Identified Weaknesses:

# State of Washington

During FY24, UW financial reporting did not complete fund level reconciliations to adequately support balances reported in the ACFR. UW does not verify that all financial statement balances are translated appropriately for state reporting. OFM did not perform sufficient procedures to verify UW balances in AFRS were accurate [F: UW consolidation, reconciliation and adjustment of balances].

## **STEP 2: Confirm Key Controls**

**Key Control 1 - UW financial reporting imports Workday financial data to AFRS on a monthly basis using text files. AFRS automatically generates error reports to identify any financial data lines that would not appropriately post. UW financial reporting will review and correct error codes to ensure data from workday is accurately uploaded.**

### Posted Transaction

To confirm Workday financial data is imported to AFRS accurately, we obtained an example of an integration file for the fiscal year 2024, for the month of May titled "FM11-MAY-Combined\_UW\_AFRS\_Transaction\_Coding-May-0708-new.xlsx". The batch was posted 6/17/2024. We selected one transaction to ensure AFRS coding was appropriately applied based on mapping documents at [UW Workday to AFRS Mapping Documents]. The transaction with linekey 15786 and accounting date of 5/1/2024 was originally posted as a credit to ledger account 10100 (claim on cash) with a ledger account summary (LAS) reference ID of LAS12135, fund reference ID of FD200, amount of \$16,877.51.

Per mapping documents, in AFRS this would be designated as:

GL 1353 due from other governments amount

Fund 145 Institutions of Higher Education - Grant and Contracts Account

We reviewed the combined data (UW Workday with appended OFM AFRS coding) and noted the transaction was posted to the expected GL and fund based on mapping documents. AFRS GL and fund appeared appropriate based on the type of transaction. We reviewed the "results" column in the integration data and noted the transaction was successfully posted. ***No issues noted.***

### Errored Transaction

To confirm error reports are reviewed by OFM and UW on a monthly basis, we obtained an example of an error report and review performed by Tina Young, Senior Financial Reporting Analyst. Error code reports are obtained by Qing Gao, OFM IT Architecture Specialist, and modified from text file to an excel file with detailed transaction data to provide to UW for their review. We obtained UW's review of error codes for the error report ran 10/08/2024. The error report, RPT DWP8002, identified 40 instances where transactions had various error codes, including E68, Subobject required.

We reviewed one transaction with error code E68 in the "summary review" tab of "ErrorCOASummaryWithUWCoding - 2024 PC4 w Descriptions." The transaction was posted to fund 148, institutions of higher education in GL account 6510, amount of \$2,367,198.43. Per UW coding this was a credit amount to 61010 for scholarships paid by 3rd party. UW identified the solution for this error code to add subobject EZ (other goods and services). The transaction was successfully posted with the solution. The solution appeared reasonable based on the error code. ***No issues noted.***

## State of Washington

We also reviewed the mapping of funds between AFRS and UW Workday to ensure that funds appeared to be appropriately mapped between the two systems. We reviewed the 90 mapped funds as of 8/12/2024 at [\[Fund Mapping Review\]](#). Fund mapping appeared reasonable. *No issues noted.*

### **Key Control 2 - UW financial reporting identifies reconciling items in fund level reconciliations provides them to OFM. Staff in UW's Financial Reporting unit prepare the fund level reconciliations for each fund and the controller reviews**

We performed a walkthrough of UW Financial Reporting's fund level reconciliation process on November 20, 2024 with Tina Young, Senior Financial Reporting Analyst. She showed us the fund level reconciliation that was in process for fund 001. Reconciling items included descriptions such as "mapping difference between rev and exp." Per OFM and UW, they do not expect to make any adjusting entries for variances or errors identified during the reconciliation since reconciliations were not completed timely. **See issue documented in conclusion above.**

### **Key Control 3 - UW financial reporting performs reconciliations of UW financial statement balances to significant ACFR balances (at request of SAO).**

We obtained natural class reconciliations for our identified significant ACFR balances included in the significant account matrix [\[Final Planning Significant Account Matrix\]](#) from Susan Stolle, Associate Controller. We reviewed the capital assets reconciliation, which included AFRS trial balance data, UW financial statement data, and a summary tab that compared the two. Per the UW financial report (note 6), buildings were reported at a net balance of \$4,105,180,000. Reported amounts in AFRS GL (2210 and 2220) totalled 4,105,178,671. The difference is due to rounding in UW's report. *No issues noted.*

We utilized UW's prepared natural class reconciliations for our testing to determine if ACFR amounts are representative UW balances from their financial report at [\[Substantive Test - AFRS Recons to UW Statements\]](#). Although UW prepares reconciliations at SAO's request, UW does not verify that all financial statement balances are translated appropriately for state reporting. **See issue in conclusion above.**

## **STEP 3: Preliminary Control Risk Assessment**

**MAX** - Internal controls are not in use. **Accordingly, we are reporting the following material weakness:**

During FY24, UW financial reporting did not complete fund level reconciliations to adequately support balances reported in the ACFR. UW does not verify that all financial statement balances are translated appropriately for state reporting. OFM did not perform sufficient procedures to verify UW balances in AFRS were accurate. See issue [\[F: UW consolidation, reconciliation and adjustment of balances\]](#).

## **STEP 4: Control Risk at LOW - Test Key Controls**

Not applicable - we are not planning on relying on controls and therefore do not need to test controls; control risk will be assessed at maximum.

## **STEP 5: Final Control Risk Assessment**



# State of Washington

**MAX** - Internal controls are not in use. **Accordingly, we are reporting the following material weakness:**

During FY24, UW financial reporting did not complete fund level reconciliations to adequately support balances reported in the ACFR. UW does not verify that all financial statement balances are translated appropriately for state reporting. OFM did not perform sufficient procedures to verify UW balances in AFRS were accurate [F: UW consolidation, reconciliation and adjustment of balances].

## K.2.PRG - Work of Other Auditors - UW

*Procedure Step:* External Auditor performs PART of audit

*Prepared By:* RKM, 11/14/2024

*Reviewed By:* SHW, 12/10/2024

### Purpose/Conclusion:

#### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

#### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for University of Washington.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted **no** concerns with the work of other auditors to bring to the attention of management at the exit conference.

### Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

# State of Washington

## **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be reviewed and incorporated into our audit as described in step 9 below.

## **ADDITIONAL procedures for SIGNIFICANT components:**

## State of Washington

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

- Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

- Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

- Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

- Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

- Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

## State of Washington

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

Component auditor has performed the audit in accordance with GAAS or GAGAS.

Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit*

# State of Washington

*Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **SAO Audit Policy [6240](#) – Group Audits**

### **[Review Work of Others](#) Planning Guide**

**[CPA Workpaper Review Resources](#)** - more background and resources for this area

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

Record of Work Done:

## **Evaluating Significance of Components Audited by Others**

We evaluated each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion units. We determined that the external CPA audit of the University of Washington is significant to the FY2024 State of Washington ACFR audit. See our analysis of which opinion units are impacted by the external audit here: [\[Rely on Work of Other Auditors\]](#).

KPMG, LLP, performed a group audit over the University of Washington and its component units. This includes the discretely presented Valley Medical Center [\[Work of Other Auditors - Valley Medical\]](#) and Fred Hutchinson Cancer Center [\[Work of Other Auditors - Fred Hutch\]](#) and a number of blended component units. The overall impact of the University of Washington audit applies to multiple opinion units in the Government Wide Financial Statements.

## **Meetings**

We determined it was not necessary to attend key meetings between KPMG and the University of Washington. We introduced ourselves to Paige Hagen, KPMG Audit Managing Director, and Casey Byers, KPMG Senior Manager, on September 17, 2024.

## **Review of SIGNIFICANT Components**

During planning, we documented in the Audit Plan and Significant Balances spreadsheet our expected reliance on the work of other auditors for

## State of Washington

significant components and the effect on our audit report and substantive testing.

### Communication with Other Auditor

As documented in [Audit Request - External Audit Coordination], we communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. We received a response on August 21, 2024 from Chris Ray, Partner [KPMG Response to SAO Letter]. We determined this response was reasonable. We arranged with Casey Byers, KPMG Senior Audit Manager, to obtain access to KPMG workpapers. Access was through the Citrix Workplace App from November 13, 2024 to November 14, 2024.

### CPA Audit Report Review

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. The auditor's work did not cover all of the State of Washington activities and was isolated to University of Washington activities only. We determined the external auditor's work was **not** done in lieu of an SAO audit. See: [Review Checklist - CPA Workpapers]. **The audit work and documentation was sufficient to allow our Office to rely on KPMG's work.**

### Evaluation of Professional Competence

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report. Based on these procedures, we determined that the professional competence of the other auditor was sufficient enough to rely on their work.

### Understanding of Consolidation Process

We gained an understanding of controls over the consolidation process as documented in [Financial Statement Preparation]. We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

### Incorporation of Results of Other Audit

We reviewed the auditor's reports [UW 2024 Audit Report], the aggregation of misstatements, any audit recommendations made and any other relevant results. To incorporate results, we:

- Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented [UW GL to AFRS Testing]. **See issues identified in the spreadsheet.**

- Looked for any uncorrected misstatements identified by the other auditor. We added these to our aggregation for the primary government. See: [Aggregation of Misstatements (GAAP)].

- Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. We noted no such matters.

- Looked for any modifications or explanatory paragraphs. We determined there were modifications or explanatory paragraphs, but this did not impact KPMG's work or our audit conclusions.

- We determined that the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

# State of Washington

## Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors was met as follows:

The audit was dated November 8, 2024, which is prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence. We specifically noted that the component auditor has passed its prior peer review.

Component financial statements are prepared using a GASB financial reporting framework.

Component auditor has performed the audit in accordance with GAGAS.

Component auditor's report is not restricted as to use.

## K.2.PR.G - Work of Other Auditors - UW

*Procedure Step:* Substantive Test - AFRS Recons to UW Statements

*Prepared By:* BM2, 12/10/2024

*Reviewed By:* RKM, 12/10/2024

Purpose/Conclusion:

### **Purpose:**

To review the Workday to AFRS roll-up of the University of Washington financial balances.

### **Source:**

Susan Stolle, Associate Controller

### **Conclusion:**

We reviewed the Workday to AFRS roll-up of the University of Washington financial balances and identified several errors due to misclassification and reconciliation variances. See issue at: [\[F: UW consolidation, reconciliation and adjustment of balances\]](#).

Testing Strategy:

Obtain the University of Washington audited financial statements.

## State of Washington

Obtain the UW performed line item reconciliations for selected balances (natural class reconciliations). Compare balances reported in the reconciliation to AFRS data, and determine if explanations are reasonable and complete for reconciling items. Determine if the reconciliations meet a reasonable threshold as to not present a risk of a material difference between the balances at UW and the AFRS balances reported.

Identify any unreconciled balances over the floor and carry them to the aggregation of misstatements as a possible error.

Guidance/Criteria:

Record of Work Done:

Risk(s) identified during planning:

Although the Universities financial statements are audited by a CPA firm, there is a risk that the adjustments made to AFRS for state reporting may be incomplete, inappropriate or inaccurate, potentially affecting assertions in the higher special revenue, higher student services and higher endowment opinion units. In addition the UW implemented a new ERP (Workday) in FY24 potentially increasing risk.

There is a risk that the data converted from Workday to AFRS is not accurate and complete.

Planned Audit Procedures from ACFR Brainstorm [[ACFR Brainstorm](#)]:

**Obtain an understanding of the process of adjusting UW accounting records and reporting in AFRS at a summary level** [[Controls - UW Workday GL to AFRS](#)]

See controls reviewed at [[Controls - UW Workday GL to AFRS](#)].

**Identify and confirm key controls over the financial reporting process and note any control weaknesses** [[Controls - UW Workday GL to AFRS](#)]

We identified a material control weakness as part of our controls related to the consolidation of UW data. See issue [[F: UW consolidation, reconciliation and adjustment of balances](#)].

We reviewed the mapping of funds from UW Workday and AFRS at [[Fund Mapping Review](#)]. Based on our review of fund descriptions and rollup funds, we determined the mapping of funds appears reasonable. *No issues noted.*

We also reviewed adjustments made after phase II close as part of our adjustment testing at [[FY24 Greater than \\$5M Adjustment Testing](#)]. **See issue in the spreadsheet.**

**Agree select line items from the UW financial statements to the state ACFR** [[UW GL to AFRS Testing](#)]



## State of Washington

We obtained natural class reconciliations from Susan Stolle, UW Associate Controller, for 23 of the 44 selected line items (from significant account matrix at B.3.1). Due to the complexity of mapping data from AFRS to Workday and our limited access to UW financial statement data, we utilized UW's reconciliations to trace UW financial statement balances back to the applicable ACFR balance. We used the ACFR database to verify amounts reported in the ACFR were representative of UW's financial statement balances reported at [\[UW 2024 Audit Report\]](#).

Based on our procedures, we identified unreconciled balances of \$2.2 billion and variances of \$3.3 million across opinion units for the 23 balances. There were 10 balances that reported variances above their applicable floor. We will carry these issues to the aggregation of misstatements [\[Aggregation of Misstatements \(GAAP\)\]](#). See issue at [\[F: UW consolidation, reconciliation and adjustment of balances\]](#).

The \$2.2 billion in unreconciled balances were mainly due to cash and investments so we performed additional procedures here: [\[Cash and Investments\]](#).

Tab 1: We ran an AFRS query to obtain the total cash and investments reported amount by UW. We compared this query to the UW reported amount per their FY24 financial statements. We determined the total cash and investments tied with an insignificant variance.

Tab 2: We ran an AFRS query to obtain the cash and investments reported amount by UW for rollup funds FBG, FEA and FFH (major funds). We assessed whether year over year cash and investment changes for rollup funds FBG, FEA and FFH appear reasonable. The balances did not significantly change so we determined they appeared reasonable.

Tab 3: We ran an AFRS query to obtain the cash and investments reported amount by UW for rollup funds FBG, FEA and FFH (major funds). We assessed whether classification of cash and investments appeared reasonable by examining year over year changes by rollup fund and GL sort code. We determined there were significant fluctuations and were unable to quantify the error for classification of cash and investment for rollup funds FBG, FEA and FFH.

### K.3.PR.G - Work of Other Auditors - SIB

*Procedure Step:* External Auditor Performing PART of Audit

*Prepared By:* JLE, 10/30/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion:

#### **Purpose**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

# State of Washington

## **Conclusion**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for the following components: The Washington State Investment Board.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted no concerns with the work of other auditors to bring to the attention of management at the exit conference.

SAO will add an Emphasis of Matter paragraph to the final ACFR report, disclosing the fair value estimation method for Retirement Funds investments.

## **No issues noted.**

Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

## **Procedures for ALL Components Audited by External Auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented*

## State of Washington

*and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be reviewed and incorporated into our audit as described in step 9 below.

### **ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

- Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

- Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

- Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

- Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

- Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA

## State of Washington

workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

## State of Washington

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

Component auditor has performed the audit in accordance with GAAS or GAGAS.

Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6240](#) – Group Audits**

**[Review Work of Others](#) Planning Guide**

**[CPA Workpaper Review Resources](#)** - more background and resources for this area

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

# State of Washington

Record of Work Done:

## **Evaluating Significance of Components Audited by Others**

We identified the following other auditors who performed a portion of the financial statement audit, and determined the significance of those components, as follows:

We evaluated each component audited by others to determine whether their work was, individually or in aggregate, significant or insignificant to applicable opinion units. See: [\[Interim Planning Significant Balance Spreadsheet\]](#).

We determined the audit of the State Investment Board (SIB) performed by external auditors **was significant** to the FY24 State of Washington ACFR audit.

We identified the following other auditors who performed a portion of the ACFR financial statement audit (i.e., the audit of SIB):

Firm Name: Eide Bailly, LLP

Audit Supervisor: Abbie Belthoff, CPA

Email: [abelthoff@eidebailly.com](mailto:abelthoff@eidebailly.com)

Phone: (208) 383-4784

Engagement Partner: Brad Berls

## **Meetings**

We determined that attending meetings between Eide Bailly and SIB was **not necessary**.

## **Review of SIGNIFICANT Components:**

During planning, we documented our expected reliance on the work of other auditors for significant components and the effect of such reliance on our audit report and substantive testing. See planning documentation at: [\[Final Planning Significant Balance Spreadsheet\]](#) and [\[External CPA Audit Significance\]](#).

## **Communication with Other Auditor**

We communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. See documentation of correspondence at: [\[Audit Request - External Audit Coordination\]](#).

We received a response on 9/26/2024 from Brad Berls, CPA (Eide Bailly Partner). See documentation of the external auditor's response at: [\[Response Letter WSIB\]](#).

We evaluated the external auditor's response, noting **no issues** relating to their understanding, cooperation, and willingness to share relevant information. Their response was complete and reasonable.

## **CPA Audit Report Review**

# State of Washington

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. See our report review here: [\[FY24 Review Checklist\]](#).

We concluded that the external auditor's work was reasonable, sufficient, conforms to relevant Standards, and can be relied upon. **No issues noted.**

## Evaluation of Professional Competence

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report.

Based on these procedures, we determined that the professional competence of the other auditor **was sufficient** enough to rely on their work.

## Understanding of Consolidation Process

We gained an understanding of controls over the consolidation process as documented in: [\[Financial Statement Preparation\]](#).

We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

## Incorporation of Results of Other Audit

We reviewed the auditor's reports, the aggregation of misstatements, any audit recommendations made, and any other relevant results.

To incorporate results, we:

Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented at: [\[FY24 Reconciliation to AFRS\]](#) and [\[FY24 DRS Retirement Strategy Funds Reconciliation\]](#).

Looked for any uncorrected misstatements identified by the other auditor. We noted there were **no uncorrected misstatements** identified by the other auditor.

Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. **We noted no such matters.**

Looked for any modifications or explanatory paragraphs, noting one Emphasis of Matter paragraph added to the report for Retirement Funds, see: [\[WSIB Annual Report 2024\]](#), page 20.

"Total investments in the Retirement Funds include investments valued at \$93.9 billion (55.5% of total investments) as of June 30, 2024, whose fair values have been estimated by management in the absence of readily determinable fair values.

Management's estimates are based on information provided by the fund managers or the general partners. Our opinion is not modified with respect to this matter."

**We will add an Emphasis of Matter paragraph to the ACFR report. See conclusion above.**

We determined that the work, materiality, performance materiality and floor thresholds used **are acceptable** for our purposes, based on our communication with the component auditor and other procedures performed.

## Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors **was met** as follows:

The audit was dated 9/26/2024, which is **prior** to our report on the primary government.

## State of Washington

There are **no concerns** about the component auditor's professional competence or independence; we specifically note that the component auditor has **passed** its most recent peer review.  
Component financial statements are prepared using a **GASB** financial reporting framework.  
Component auditor has performed the audit in accordance with **GAGAS**.  
Component auditor's report **is not** restricted as to use.

**SAO will make reference to the attestation work of other auditors as performed for the State Investment Board (a significant component of the FY24 Washington State ACFR). No issues noted.**

### K.4.PRG - Work of Other Auditors - DRS

*Procedure Step:* External Auditor performs PART of audit  
*Prepared By:* BFW, 11/4/2024  
*Reviewed By:* RKM, 11/5/2024

#### Purpose/Conclusion:

##### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

##### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for Department of Retirement Systems.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted **no** concerns with the work of other auditors to bring to the attention of management at the exit conference.

#### Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit



# State of Washington

Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

## **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be

## State of Washington

reviewed and incorporated into our audit as described in step 9 below.

### **ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

- Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

- Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

- Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

- Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

- Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to

## State of Washington

obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

## State of Washington

Component auditor has performed the audit in accordance with GAAS or GAGAS.  
Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6240](#) – Group Audits**

**[Review Work of Others](#) Planning Guide**

**[CPA Workpaper Review Resources](#)** - more background and resources for this area

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

Record of Work Done:

### **Evaluating Significance of Components Audited by Others**

We identified the following other auditors who performed a portion of the financial statement audit and determined the significance of those components as follows: UHY LLP

We determined that the external CPA audit of the Department of Retirement Systems is significant to the FY24 State of Washington ACFR. See our analysis of which opinion units are impacted by the external audit here: [\[External CPA Audit Significance\]](#)

### **Meetings**

We considered participation in meetings between the external auditor (UHY LLP) and the Department of Retirement systems and determined it was not necessary.

### **Review of SIGNIFICANT Components**

During planning, we documented in the Audit Plan and Significant Balances spreadsheet our expected reliance on the work of other auditors for

## State of Washington

significant components and the effect on our audit report and substantive testing.

### Communication with Other Auditor

As documented in [\[Audit Request - External Audit Coordination\]](#), we communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. We received a response on August 15, 2024 from Jason Ostroski, Principal [\[RE Audit Request - External Audit Coordination\]](#). We determined the response was reasonable.

We arranged with Ivana Ritz, Manager, to obtain access to UHY LLP workpapers. Access was through the Splashtop browser from October 28, 2024 to October 30, 2024.

### CPA Audit Report Review

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. The auditor's work did not cover all of the State of Washington activities and was isolated to DRS funds only. We determined the external auditor's work was **not** done in lieu of an SAO audit. We determined a CPA audit report review required under SAO Audit Policy 3510 was not applicable. See our review of the CPA workpapers here: [\[Review Checklist - CPA Workpapers\]](#). **We determined the work and documentation was sufficient to allow our Office to rely on the work of UHY LLP.**

### Evaluation of Professional Competence

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report. Based on these procedures, we determined that the professional competence of the other auditor was sufficient enough to rely on their work.

### Understanding of Consolidation Process

We gained an understanding of controls over the consolidation process as documented in [\[Financial Statement Preparation\]](#). We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

### Incorporation of Results of Other Audit

We reviewed the auditor's reports [\[2024-ACFR\]](#), [\[FY24 DRS Report\]](#), [\[DRS Internal Control Report\]](#), the aggregation of misstatements, any audit recommendations made and any other relevant results. To incorporate results, we:

- Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented [\[FY24 DRS Reconciliation to AFRS\]](#).

- We noted there were no uncorrected misstatements identified by the other auditor.

- Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. We noted no such matters.

- Looked for any modifications or explanatory paragraphs. We noted no such matters.

- We determined that the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

# State of Washington

## Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors was **met** as follows:

The audit was dated October 24, 2024, which is prior to our report on the primary government.

There are **no** concerns about the component auditor's professional competence or independence. We specifically noted that the component auditor has **passed** its prior peer review.

Component financial statements are prepared using a GASB financial reporting framework.

Component auditor has performed the audit in accordance with GAGAS.

Component auditor's report **is not** restricted as to use.

## Auditor Note:

In the fall of 2021, DRS Retirement Strategy Funds (RSFs) began incorporating a sliver of the TAP into their various vintages. RSFs are provided by WSIB. DRS has always recorded the RSFs (in total) in their records. WSIB has to account for their ownership and allocates income from the TAP to maintain the pool of owners and reports this on their financial statements. They do not book these balances in AFRS. DRS pools DC and DCP funds, including total RSF balances, and books them to AFRS. We documented this change in our review of the WSIB audited financial statements [[FY24 Reconciliation to AFRS](#)] and the rely on work of others step here: [[Work of Other Auditors - SIB](#)]. This change does not affect our ability to rely on the other auditor's work for either WSIB or DRS.

## K.4.PRG - Work of Other Auditors - DRS

*Procedure Step:* Reivew of PEFI

*Prepared By:* BFW, 10/30/2024

*Reviewed By:* RKM, 11/5/2024

Purpose/Conclusion.*
----------------------

## **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant allocations.

## **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors.

## State of Washington

We noted **no** concerns with the work of other auditors to bring to the attention of management at the exit conference.

### Testing Strategy:

We will identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant allocations.

### Guidance/Criteria:

### Record of Work Done:

#### **Review of PEFI Workpapers**

We reviewed the workpapers for the 06/30/2024 PEFI report [2024 PEFI] prepared by DRS and audited by UHY LLP. The PEFI audit report was prepared under AU-C section 805, *Special Considerations* – Audits of Single Financial Statements and Specific Elements, Accounts, or Items of a Financial Statement. Due to the nature of AU-C 805 engagement, we elected to not use the CPA workpaper review checklist to ensure we gained sufficient understanding over testing performed over census data and allocations (unique elements of an AU-C 805 engagement). Our review included documenting the following:

- Review planning,
- Control work,
- Substantive work,
- Work performed on the report, and
- Conclusion over workpapers.

See the checklist used and documentation of our workpaper review at [PEFI Review Checklist - CPA Workpapers]. We also noted materiality was considered for each pension balance by plan. See documentation of planning materiality, performance materiality, individually significant items threshold, and each floor at [PEFI Materiality Threshold 2024]. We noted the following:

- Conclusions at the workpaper level supported the opinion,
- Engagement risks were appropriately addressed,
- Sufficient procedures were performed over census data, allocation basis and percentages reported, and

We determined we can rely on the auditors' work for the FYE 2024 PEFI.

#### **K.5.PR.G - Work of Other Auditors - LGIP**

# State of Washington

*Procedure Step:* External Auditor performs PART of audit  
*Prepared By:* EJB, 11/5/2024  
*Reviewed By:* RKM, 11/7/2024

## Purpose/Conclusion:

### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for the Local Government Investment Pool.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted no concerns with the work of other auditors to bring to the attention of management at the exit conference.

## Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

### **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on*



## State of Washington

*the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be reviewed and incorporated into our audit as described in step 9 below.

### **ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

## State of Washington

Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

## State of Washington

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

Component auditor has performed the audit in accordance with GAAS or GAGAS.

Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

# State of Washington

## SAO Audit Policy [6240](#) – Group Audits

### [Review Work of Others](#) Planning Guide

[CPA Workpaper Review Resources](#) - more background and resources for this area

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

Record of Work Done:

#### **Evaluating Significance of Components Audited by Others**

We evaluated each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion units.

We determined that the external CPA audit of the Office of the State Treasurer - Local Government Investment Pool is significant to the FY24 State of Washington ACFR audit. See our analysis of which opinion units are impacted by the external audit here: [\[External CPA Audit Significance\]](#).

#### **Meetings**

We concluded that it was not necessary to attend meetings.

#### **Review of SIGNIFICANT Components**

During planning, we documented in the Audit Plan and Significant Balances spreadsheet our expected reliance on the work of other auditors for significant components and the effect on our audit report and substantive testing.

#### **Communication with Other Auditor**

As documented in [\[Audit Request - External Audit Coordination\]](#), we communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. We received a response from Kory Hoggan, Partner [\[WA SAO Letter 7.30.24\]](#).

We arranged with Kory Hoggan, Partner, to obtain access to Moss Adams LLP workpapers. Access was through the Citrix Gateway Desktop browser on November 5, 2024.

#### **CPA Audit Report Review**

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. See workpaper review at

## State of Washington

[[Review Checklist - CPA Workpapers](#)]. The auditor's work did not cover all of the State of Washington activities and was isolated to LGIP only. We determined the external auditor's work was **not** done in lieu of an SAO audit. **We noted no concerns and determined we could rely on the auditor's work.**

### Evaluation of Professional Competence

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report. Based on these procedures, we determined that the professional competence of the other auditor was sufficient enough to rely on their work.

### Understanding of Consolidation Process

We gained an understanding of controls over the consolidation process as documented at [[Financial Statement Preparation](#)]. We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

### Incorporation of Results of Other Audit

We reviewed the auditor's reports [[LGIP Audited FS - 2024](#)], [[WA LGIP AU 260 Memo 6.30.24](#)], [[WA LGIP GAGAS IC Report 6.30.24](#)], the aggregation of misstatements, any audit recommendations made and any other relevant results. To incorporate results, we:

- Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented at [[LGIP Reconciliation to AFRS - 2024](#)].

- Looked for any uncorrected misstatements identified by the other auditor. We noted there were no uncorrected misstatements identified by the other auditor.

- Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. We noted no such matters.

- Looked for any modifications or explanatory paragraphs. There is an emphasis of matter paragraph in the audit report. This paragraph notes that the audit report covers the LGIP only, and not the Office of the State Treasurer or the State of Washington. No other modifications to the report were noted.

- We determined that the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

### Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors was **met** as follows:

- The audit was dated October 15, 2024, which is prior to our report on the primary government.

- There are **no** concerns about the component auditor's professional competence or independence. We specifically noted that the component auditor has **passed** its prior peer review.

- Component financial statements are prepared using a GASB financial reporting framework.

- Component auditor has performed the audit in accordance with GAGAS.

- Component auditor's report **is not** restricted as to use.

# State of Washington

## K.6.PRG - Work of Other Auditors - Fred Hutch

*Procedure Step:* External Auditor performs PART of audit

*Prepared By:* EZM, 11/18/2024

*Reviewed By:* RKM, 11/19/2024

### Purpose/Conclusion:

#### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

#### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for Fred Hutchinson Cancer Center.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted no concerns with the work of other auditors to bring to the attention of management at the exit conference.

### Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

#### **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

# State of Washington

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be reviewed and incorporated into our audit as described in step 9 below.

## **ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

## State of Washington

Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.  
Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.  
Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.  
Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.  
Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).



## State of Washington

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

Component auditor has performed the audit in accordance with GAAS or GAGAS.

Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria.*
---------------------

# State of Washington

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6240](#) – Group Audits**

**[Review Work of Others](#) Planning Guide**

**[CPA Workpaper Review Resources](#)** - more background and resources for this area

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

Record of Work Done:

## **Evaluating Significance of Components Audited by Others**

We evaluated each component audited by other auditors to determine whether their work was, individually or in aggregate, significant or insignificant to applicable opinion units, see: [\[Rely on Work of Other Auditors\]](#) and [\[External CPA Audit Significance\]](#). We determined the audit of the Fred Hutchinson Cancer Center (FHCC) performed by external auditors **was significant** to the fiscal year end June 30, 2024 State of Washington ACFR audit.

We identified the following other auditors who performed a portion of the financial statement audit (audit of FHCC):

KPMG

Parker Olinger

Email: polinger@KPMG.com

Phone: (360) 597-8198

Engagement Partner: Brad Berls

## **Meetings**

We did not find it necessary to attend the meetings between FHCC staff and KPMG.

## **Review of SIGNIFICANT Components**

During planning, we documented in the Audit Plan and Significant Balances spreadsheet our expected reliance on the work of other auditors for significant components and the effect on our audit report and substantive testing.

# State of Washington

We noted no red flags for consideration in our financial statement audit

## Communication with Other Auditor

As documented in [\[Audit Request - External Audit Coordination\]](#), we communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. We received a response on September 12, 2024 from Parker Olinger, Senior Audit Manager at KPMG LLP [\[RE Audit Request - External Audit Coordination\]](#). We arranged with Parker to obtain access to KPMG workpapers. Access was through the Citrix Workplace App from October 29, 2024 through October 30, 2024.

Response received was within our expectation.

## CPA Audit Report Review

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. The auditor's work did not cover all of the State of Washington activities and was isolated to Fred Hutchinson Cancer Center activities only. We determined the external auditor's work was **not** done in lieu of an SAO audit. See our review of the CPA workpapers here: [\[Review Checklist - CPA Workpapers\]](#). **We determined the work and documentation was sufficient to allow our Office to rely on the work of KPMG LLP.**

## Evaluation of Professional Competence

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report. Based on these procedures, we determined that the professional competence of the other auditor was sufficient enough to rely on their work.

## Understanding of Consolidation Process

We gained an understanding of controls over the consolidation process as documented in [\[Controls - FS Preparation\]](#). We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

## Incorporation of Results of Other Audit

We reviewed the auditor's reports [\[FHCC Audit Report\]](#), and letter to management and the governing body about internal controls (pg. 39), the aggregation of misstatements, any audit recommendations made and any other relevant results. To incorporate results, we:

- Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented [\[Component Unit Financial Statements\]](#).

- We noted there were no uncorrected misstatements identified by the other auditor.

- Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. We noted no such matters.

- Looked for any modifications or explanatory paragraphs. We noted no such matters.

- We determined that the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

# State of Washington

## Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors was **met** as follows:

The audit was dated October 16, 2024, which is prior to our report on the primary government.

There are **no** concerns about the component auditor's professional competence or independence. We specifically noted that the component auditor has **passed** its prior peer review.

Component financial statements are prepared using a GASB financial reporting framework.

Component auditor has performed the audit in accordance with **GAGAS**.

Component auditor's report **is not** restricted as to use.

## K.7.PRG - Work of Other Auditors - Health Benefit Exchange

*Procedure Step:* External Auditor performs PART of audit

*Prepared By:* EJB, 11/13/2024

*Reviewed By:* RKM, 11/19/2024

Purpose/Conclusion:

### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for the Washington Health Benefit Exchange.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted no concerns with the work of other auditors to bring to the attention of management at the exit conference.

Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit

# State of Washington

Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

## **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be

## State of Washington

reviewed and incorporated into our audit as described in step 9 below.

### **ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

- Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

- Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

- Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

- Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

- Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to

## State of Washington

obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

# State of Washington

Component auditor has performed the audit in accordance with GAAS or GAGAS.  
Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:

## **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **SAO Audit Policy [6240](#) – Group Audits**

### **[Review Work of Others](#) Planning Guide**

**[CPA Workpaper Review Resources](#)** - more background and resources for this area

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

Record of Work Done:

## **Evaluating Significance of Components Audited by Others**

We evaluated each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion units.

We determined that the external CPA audit of the Washington Health Benefit Exchange (WHBE) is significant to the FY24 State of Washington ACFR audit. See our analysis of which opinion units are impacted by the external audit here: [\[External CPA Audit Significance\]](#).

## **Meetings**

We concluded that it was not necessary to attend meetings.

## **Review of SIGNIFICANT Components**

During planning, we documented in the Audit Plan and Significant Balances spreadsheet our expected reliance on the work of other auditors for



## State of Washington

significant components and the effect on our audit report and substantive testing.

### Communication with Other Auditor

As documented in [\[Audit Request - External Audit Coordination\]](#), we communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. We received a response from Mark LaPrade, Partner [\[RE Audit Request - HBE External Audit Coordination\]](#).

We arranged with Nathan Dunlap, Senior Manager, to obtain access to BerryDunn's workpapers. Access was through Zoom on November 11, 2024 and November 13, 2024.

### CPA Audit Report Review

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. See workpaper review at [\[Review Checklist - CPA Workpapers\]](#). The auditor's work did not cover all of the State of Washington activities and was isolated to WHBE only. We determined the external auditor's work was **not** done in lieu of an SAO audit. **We noted no concerns and determined we could rely on the auditor's work.**

### Evaluation of Professional Competence

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report. Based on these procedures, we determined that the professional competence of the other auditor was sufficient enough to rely on their work.

### Understanding of Consolidation Process

We gained an understanding of controls over the consolidation process as documented at [\[Financial Statement Preparation\]](#). We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

### Incorporation of Results of Other Audit

We reviewed the auditor's reports [\[Washington Health Benefit Exchange 2024 Financial Statements FINAL\]](#), the aggregation of misstatements, any audit recommendations made and any other relevant results. To incorporate results, we:

- Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented at [\[Component Unit Financial Statements\]](#).

- Looked for any uncorrected misstatements identified by the other auditor. We noted there were no uncorrected misstatements identified by the other auditor.

- Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. We noted no such matters.

- Looked for any modifications or explanatory paragraphs.

## State of Washington

There is a "Other Reporting Required by *Government Auditing Standards* paragraph at the bottom of the audit report. This paragraph details another report issued on the consideration of the Exchange's internal control over financial reporting and on their tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements and other matters. There was no opinion issued on the effectiveness of internal control or on compliance.

We determined that the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

### Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors was **met** as follows:

The audit was dated October 29, 2024, which is prior to our report on the primary government.

There are **no** concerns about the component auditor's professional competence or independence. We specifically noted that the component auditor has **passed** its prior peer review.

Component financial statements are prepared using a GASB financial reporting framework.

Component auditor has performed the audit in accordance with GAGAS.

Component auditor's report **is not** restricted as to use.

### K.8.PR.G - Work of Other Auditors - Valley Medical

*Procedure Step:* External Auditor performs PART of audit

*Prepared By:* DRR, 10/14/2024

*Reviewed By:* RKM, 11/19/2024

Purpose/Conclusion.*
----------------------

#### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

#### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for Valley Medical Center.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

# State of Washington

We noted no concerns with the work of other auditors to bring to the attention of management at the exit conference.

## Testing Strategy:

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

### **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a*

## State of Washington

*letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be reviewed and incorporated into our audit as described in step 9 below.

### **ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

- Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

- Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

- Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

- Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

- Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

## State of Washington

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to

## State of Washington

reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

Component auditor has performed the audit in accordance with GAAS or GAGAS.

Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

### **SAO Audit Policy [6240](#) – Group Audits**

### **[Review Work of Others](#) Planning Guide**

### **[CPA Workpaper Review Resources](#) - more background and resources for this area**

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

Record of Work Done:

### **Evaluating Significance of Components Audited by Others**

We evaluated each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion units. We determined that the external CPA audit of the Valley Medical Center (VMC) is significant to the FY2024 State of Washington ACFR audit. See our analysis of which opinion units are impacted by the external audit here: [[Interim Planning Significant Balance Spreadsheet](#)].

## State of Washington

We identified the following other auditors who performed a portion of the financial statement audit (Valley Medical Center Audit):

KPMG, LLC:

Casey Byers, Audit Manager

Phone: (206) 913-4147

Email: jamesbyers@kpmg.com

### **Meetings**

We did not find it necessary to attend the meetings between Valley Medical staff and KPMG.

### **Review of SIGNIFICANT Components**

During planning, we documented in the Audit Plan and Significant Balances spreadsheet our expected reliance on the work of other auditors for significant components and the effect on our audit report and substantive testing.

We noted no red flags for consideration in our financial statement audit

### **Communication with Other Auditor**

As documented in [[Audit Request - External Audit Coordination](#)], we communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. We received a response on July 26, 2024 from Casey Byers, Audit Manager at KPMG, LLC [[RE Audit Request - External Audit Coordination](#)]. We arranged with Casey Byers, Audit Manager, to obtain access to KPMG workpapers. Access was through the Citrix Workplace App from October 2, 2024 through October 3, 2024.

Response received was within our expectation.

### **CPA Audit Report Review**

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. The auditor's work did not cover all of the State of Washington activities and was isolated to Valley Medical Center activities only. We determined the external auditor's work was **not** done in lieu of an SAO audit. See our review of the CPA workpapers here: [[Review Checklist - CPA Workpapers](#)]. **We determined the work and documentation was sufficient to allow our Office to rely on the work of KPMG LLC.**

### **Evaluation of Professional Competence**

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report. Based on these procedures, we determined that the professional competence of the other auditor was sufficient enough to rely on their work.

### **Understanding of Consolidation Process**

## State of Washington

We gained an understanding of controls over the consolidation process as documented in [\[Controls - FS Preparation\]](#). We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

### Incorporation of Results of Other Audit

We reviewed the auditor's reports, [\[VMC - Financial Statements\]](#) and letter to management and the governing body about internal controls [\[VMC - Report on Internal Controls\]](#), the aggregation of misstatements, any audit recommendations made and any other relevant results. To incorporate results, we:

Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented [\[Component Unit Financial Statements\]](#).

Looked for any uncorrected misstatements identified by the other auditor and we noted there were no uncorrected misstatements identified by the other auditor.

Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. We noted no such matters.

Looked for any modifications or explanatory paragraphs. We noted no such matters.

We determined that the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

### Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors was met as follows:

The audit was dated **September 20, 2024**, which is prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence. We specifically noted that the component auditor has **passed** its prior peer review.

Component financial statements are prepared using a GASB financial reporting framework.

Component auditor has performed the audit in accordance with GAGAS.

Component auditor's report is **not** restricted as to use.

### K.9.PRG - Work of Other Auditors - WA Housing Finance

*Procedure Step:* External Auditor performs PART of audit

*Prepared By:* BFW, 11/13/2024

*Reviewed By:* RKM, 11/19/2024



# State of Washington

## Purpose/Conclusion.

### **Purpose:**

To identify and evaluate work done by external auditors and determine if our Office can rely on audit reports issued by external auditors for significant components.

### **Conclusion:**

Based on our evaluation, we determined that our Office can rely on the work of external auditors for WA Housing Finance.

Results of the work of other auditors was identified and incorporated into other sections as described in the ROWD below.

We noted **no** concerns with the work of other auditors to bring to the attention of management at the exit conference.

## Testing Strategy.

Group audit procedures are required for all components audited by other CPAs, with certain additional procedures required only for significant components. This work should be charged to time code CPAR. If significant components are audited by CPAs in lieu of an SAO audit, a CPA Audit Report Review will also be needed in accordance with Policy 3510 and charged to time code CPAP - in such cases, some procedures in this section may be documented as part of the report review. Contact your supervisor and Assistant Director if you have any questions about necessary procedures or any concerns about the external auditor's professional reputation, independence, or quality of work.

### **Procedures for ALL components audited by external auditors:**

The following procedures are **required** for planning purposes as referenced in the "Audits Performed by Others" step and by Audit Policy 6240 to identify relevant work done by external auditors and consider results:

**STEP 1: Determine Significance to the applicable opinion unit.** Evaluate each component audited by others to determine whether - individually or in aggregate - it is significant or insignificant to the applicable opinion unit.

*Auditors should consider both quantitative and qualitative materiality factors. For example, a component may be significant based on the quantitative materiality threshold for the applicable opinion unit or because it may include significant risk of material misstatement of the primary government's financial statements due to its specific nature or circumstances. When a component represents an entire opinion unit, it is considered to be significant (with the possible exception of foundations – see special guidance for GASB 39 situations in FYI 2016-02).*

*Qualitative factors may include that a waiver to perform the review has been used in recent audits, increasing the risk where we decide it is appropriate to review the CPA workpapers to sufficiently reduce audit risk.*

# State of Washington

*Important Note: If a component is significant, communication with the other auditor (Step 5), must be done on a timely basis. In that case, Steps 2 and 3 may need to be done before the primary government's audit, as well. The results should be documented and placed in the FAWF pending the start of the SAO audit, and then brought into the TeamMate audit file.*

**STEP 2: Meetings. Consider** attending key meetings between the external auditor and the government.

**STEP 3: Obtain Report.** Include a copy of the external auditor's report in TeamMate. Make sure to get both the report on compliance and internal controls (SAO's "I-report"), as well as the financial statement report (SAO's "F-report").

*NOTE: If the other auditor performs the audit and reports in accordance with GAAS rather than GAGAS, then the I-report content will be in a letter to management rather than a report. This is possible for audits of component units (e.g. foundations or tax credit partnerships), but is not expected for divisions or funds of primary governments.*

**STEP 4: Review Report.** For insignificant components, review the report issued by external auditors and consider whether any information in the report changes our planning decisions or would have an impact on our audit, if the report is available before our report date. If questions or potential red flags are noted, **consider** additional inquiry, analysis or other steps to follow up. For significant components, the report must be reviewed and incorporated into our audit as described in step 9 below.

## **ADDITIONAL procedures for SIGNIFICANT components:**

The following additional procedures are **required** only for significant components audited by external auditors:

**STEP 5: Communication with Other Auditor.** Using the External Audit Coordination email template in the TeamStore (be sure to add your formal signature to the bottom of the email prior to sending), communicate with the external auditor to:

- Confirm the external auditor's independence, cooperation and understanding of how we intend to use their work.

- Share related parties and significant risks we have identified for the primary government and request the same from the external auditor.

- Request the external auditor's materiality and performance materiality thresholds used to determine whether thresholds are sufficient for purposes of our audit.

- Request the external auditor's report and other results in order to incorporate these into our results for the audit of the group.

- Confirm our commitment to inform the external auditor of any matter that comes to our attention that may be relevant to their audit and request the external auditor's commitment to do the same.

*Auditors should initiate this communication as early in the audit as possible and continue to communicate with the external auditor as*

# State of Washington

*necessary to follow-up on these matters throughout the audit.*

Note: if the CPA Audit Report Review is being done in step 6 below, information from the CPA can be documented when completing the CPA workpaper review checklist rather than as a response to the letter.

**STEP 6: CPA Audit Report Review (if applicable under Policy 3510).** For significant components that are audited by an external auditor in lieu of an SAO audit, perform a CPA Audit Report Review in a separate TM file as required by Policy 3510. This work is performed to carry out SAO's statutory mandate but will also provide additional support for our reliance on the work of the other auditor. As such, the review should be completed prior to concluding on the audit of the primary government. If a review is applicable, reference this work and summarize relevant results.

**STEP 7: Audit Plan.** Document in the Audit Plan the effect of the work of external auditors on our audit report and substantive testing. Identify which opinion units and/or balances we plan to rely on the work of other auditors in the plan and mark these rows or columns on the Material Balance spreadsheet to indicate our reliance on the work of external auditors.

**STEP 8: Evaluate the Firm's Professional Competence.** Evaluate the professional competence of the external audit firm by considering our Office's experience with the firm, the results of communications and review, and by checking the [CPA License and Peer Review SharePoint page](#) to obtain the firm's last peer review report.

Note: if the CPA Audit Report Review was completed using step 6 above, this evaluation can be documented when completing the CPA workpaper review checklist.

**STEP 9: Internal Controls.** Document an understanding of controls over the consolidation process to incorporate components into the financial statements in the Controls - FS Preparation step in the permanent file (or a separate step if the process is identified as its own control system due to risk or complexity).

**STEP 10: Incorporate Results.** In addition to the external auditor's report, obtain and review any letter to management and the governing body about internal controls, the aggregation of misstatements, any audit recommendations made and any other relevant results.

Items included in the external auditor's aggregation of misstatements should also be included in our aggregation for the primary government.

Reported amounts and disclosures audited by the external auditor per their report should be traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified by the external auditor should be re-evaluated for the primary government.

## State of Washington

Our report may need to reflect any modifications made to the external auditor's report (that is, if the opinion is not unmodified or includes explanatory paragraphs) and any significant deficiencies or material weaknesses reported by the external auditor. Such issues should be repeated in our report to the extent they are material to an opinion unit.

*REMINDER: When external auditors conduct their audit in accordance with GAGAS, any findings will be communicated in their audit report. Otherwise, if conducted in accordance with GAAS, any findings will be communicated to management and the governing body in a separate letter that we will need to request.*

Auditors should conclude on whether the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

**STEP 11: Conditions for Referencing the Other Auditor's Report.** Determine if the following conditions are met. If so, we will be able to reference the work of the external auditor in our report. If not, contact TAS for assistance.

The audit is completed prior to our report on the primary government.

There are no concerns about the component auditor's professional competence or independence, and the component auditor has passed its prior peer review.

Component financial statements are prepared using the same financial reporting framework as the group, or one permitted by that framework. For example, GASB provides for inclusion of FASB components.

Component auditor has performed the audit in accordance with GAAS or GAGAS.

Component auditor's report is not restricted as to use.

*If the work of the external auditor is material to any opinion unit, our financial report must refer to the external auditors - please refer to the Audit Report Standards (ARS) Manual for opinion modifications. If the external auditor performed their audit in accordance with GAAS, rather than GAGAS, our audit report will need to be further modified as shown in the ARS example.*

Guidance/Criteria:
--------------------

### **ADDITIONAL BACKGROUND**

Auditors should consider the following background information and resources when performing work on this area.

**SAO Audit Policy [6240](#) – Group Audits**

**[Review Work of Others](#) Planning Guide**

**[CPA Workpaper Review Resources](#)** - more background and resources for this area

# State of Washington

Contact the CPA Audit Coordinator or TAS with any questions or advice on required procedures or if the team is uncertain whether a CPA Report Review is applicable.

Record of Work Done:

## **Evaluating Significance of Components Audited by Others**

We identified the following other auditors who performed a portion of the financial statement audit and determined the significance of those components as follows: Eide Bailly LLP

We determined that the external CPA audit of the WA Housing Finance is significant to the FY24 State of Washington ACFR. See our analysis of which opinion units are impacted by the external audit here: [\[External CPA Audit Significance\]](#)

## **Meetings**

We considered participation in meetings between the external auditor (Eide Bailly LLP) and the WA Housing Finance and determined it was not necessary.

## **Review of SIGNIFICANT Components**

During planning, we documented in the Audit Plan and Significant Balances spreadsheet our expected reliance on the work of other auditors for significant components and the effect on our audit report and substantive testing.

## **Communication with Other Auditor**

As documented in [\[Audit Request - External Audit Coordination\]](#), we communicated with the external auditor to confirm an understanding with them, share relevant information, and provide a basis for cooperation. We received a response on September 13, 2024 from Kevin Smith, Audit Partner [\[RE Audit Request - External Audit Coordination\]](#). No issues noted.

We arranged with Kevin Smith, Audit Partner, to obtain access to Eide Bailly workpapers. Access was through the Citrix browser from November 12, 2024 to November 13, 2024.

## **CPA Audit Report Review**

SAO Audit Policy 3510 requires a CPA Audit Report Review when significant audit work is done in lieu of an SAO audit. The auditor's work did not cover all of the State of Washington activities and was isolated to WSHFC funds only. We determined the external auditor's work was **not** done in lieu of an SAO audit. See our review of the CPA workpapers here: [\[Review Checklist - CPA Workpapers\]](#). **We determined the work and documentation was sufficient to allow our Office to rely on the work of Eide Bailly LLP.**

## **Evaluation of Professional Competence**

## State of Washington

We evaluated the professional competence of the other auditor by considering our Office's experience with the firm, communication and review procedures as described above, and reading the firm's last peer review report. Based on these procedures, we determined that the professional competence of the other auditor was sufficient enough to rely on their work.

### Understanding of Consolidation Process

We gained an understanding of controls over the consolidation process as documented in [\[Financial Statement Preparation\]](#). We considered this understanding when assessing risk and in procedures performed to incorporate the results of the other audit.

### Incorporation of Results of Other Audit

We reviewed the auditor's reports [\[WSHFC Report\]](#), letter to management and the governing body about internal controls [\[WSHFC Governance Letter\]](#), the aggregation of misstatements, any audit recommendations made and any other relevant results. To incorporate results, we:

Traced reported amounts and disclosures audited by the external auditor per their report to the financial statements of the primary government as documented [\[Component Unit Financial Statements\]](#). **See issues identified in the O.6.PRG.**

We noted there were no uncorrected misstatements identified by the other auditor.

Looked for any potential fraud, noncompliance, abuse or other matters identified by the other auditor. We noted no such matters.

Looked for any modifications or explanatory paragraphs. We noted no such matters.

We determined that the work, materiality, performance materiality and floor thresholds used are acceptable for our purposes, based on our communication with the component auditor and other procedures performed.

### Making Reference to Work of Other Auditors

Finally, we determined that conditions for making reference to the work of other auditors was met as follows:

The audit was dated October 31, 2024, which is prior to our report on the primary government.

There are **no** concerns about the component auditor's professional competence or independence. We specifically noted that the component auditor has **passed** its prior peer review.

Component financial statements are prepared using a GASB financial reporting framework.

Component auditor has performed the audit in accordance with **GAAS**.

We will modify our audit report to state that the Washington State Housing Finance Commission was not audited in accordance with Government Auditing Standards.

Component auditor's report **is not** restricted as to use.

### L.1.PRG - Rely on Work of Other SAO Audits

*Procedure Step:*      Summary of Other SAO Work

# State of Washington

*Prepared By:* CJM, 11/19/2024

*Reviewed By:* CJG, 12/5/2024

## Purpose/Conclusion:

### **Purpose:**

To determine needed coordination of work performed as separate SAO financial audits.

### **Conclusion:**

The Workers Compensation Program (Fund of the Department of Labor & Industries) audit is significant to the State financial statements and will be evaluated and relied upon in the following step [Rely on Other SAO Work]. No reliance will be placed on the other audits noted because they were insignificant, did not cover FY24 or won't be completed by the state ACFR opinion date. Planned audit procedures for agencies and accounts balances selected for audit in the planning lead sheet and material account matrix will provide sufficient evidence without considering the results of these audits. **No issues noted.**

## Testing Strategy:

Perform the following procedures to determine areas of the State audited by other SAO auditors and perform additional procedures to ensure these audits can be relied upon:

- Perform a search of state agencies receiving financial statement audits as separate SAO engagements by searching for financial statement audit reports of state agencies issued after 7/1/2023.

- For each identified engagements, refer to planning steps to determine whether it is a material component using qualitative and quantitative considerations.

## Guidance/Criteria:

## Record of Work Done:

We performed the following procedures to determine areas of the State audited by other auditors and performed the referenced procedures to ensure these audits can be relied upon:

### **Identify all financial statement audits performed on ACFR components as separate SAO engagements**

We performed a search of state agencies receiving financial statement audits as separate SAO engagements by searching for financial statement audit reports of state agencies issued after 7/1/2023. See: [FY24 Other SAO Audits]

# State of Washington

**For each identified engagements, refer to planning steps to determine whether it is a material component using qualitative and quantitative considerations**

Using the materiality worksheet prepared in the planning phase of the audit at: [[Final Planning Significant Balance Spreadsheet](#)] and the major fund determination spreadsheet at: [[Major Fund Calculation](#)]. We determined only the Workers Compensation Fund (Department of Labor & Industries) was significant to the state financial statements.

For the Workers Compensation Program audit see the following procedure: [[Rely on Other SAO Work](#)]. For other agencies noted, we are not aware of any issues or uncertainties that existed as of the opinion date that could be significant to the ACFR audit.

## **L.1.PRG - Rely on Work of Other SAO Audits**

*Procedure Step:* Rely on Other SAO Work

*Prepared By:* CJM, 11/20/2024

*Reviewed By:* CJG, 12/5/2024

Purpose/Conclusion:

**Purpose:**

To ensure adequate communication and coordination on work performed separately by SAO on a component of the primary government.

**Conclusion:**

We ensured adequate communication and coordination on work performed separately by SAO on a component of the primary government. We tied the Workers' Compensation fund in the 2024 State ACFR to the audited FY24 Workers' Compensation Fund financial statements. **No issues noted.**

Testing Strategy:

To ensure adequate communication and coordination of work performed as a separate engagement by SAO on components, auditors are



## State of Washington

**required** to perform the following procedures:

Document in the Audit Plan the effect of the work performed as a separate engagement by SAO. Identify which opinion units and/or balances we plan to rely on this other work and mark the applicable rows or columns on the Material Balance spreadsheet to indicate our reliance.

Ensure communication of the following:

Related parties identified

Significant risks and any other relevant matters identified

Materiality and tolerable misstatement thresholds used.

Any indicators of possible management bias regarding accounting estimates and the application of accounting principles.

Other matters that may be relevant to the primary government's audit, such as exceptions noted in the component's management representation letter.

Audit results

Review the results of separately performed work and incorporate results into the audit of the primary government, including the following, as applicable:

Aggregation of misstatements

Significant difficulties or disagreements

Reported amounts and disclosures audited in other work traced to the financial statements of the primary government.

Any potential fraud, noncompliance, abuse or other matters identified should be re-evaluated for the primary government.

Any report modifications, significant deficiencies or material weaknesses to the extent they are material to the primary government.

*We will not make reference to other SAO audits in our audit report.*

Guidance/Criteria.:

### **ADDITIONAL BACKGROUND**

# State of Washington

Auditors should consider the following background information and resources when performing work on this area.

## SAO Audit Policy [6240](#) – Group Audits

Record of Work Done:

### **Labor and Industries ACFR - Workers' Compensation Fund (WCF)**

The FY24 SAO audit of Workers' Compensation Program (WCP) financial statements will be relied upon to provide audit coverage for the Workers' Compensation major fund opinion unit. Significant account balances and all audit tests are documented within the WCP audit. See: [TeamMate file - S1WorkersCompensation Funds-FS24]. The audit was performed by Team Financial Audit.

We documented in the Audit Plan the effect of the work performed as a separate engagement by SAO. We identified the opinion units and/or balances we planned to rely on the work of others for and marker the applicable rows or columns on the Significant Balance spreadsheet to indicate our reliance.

We noted there was adequate communication of the following:

- Related parties identified.

- Significant risks and any other relevant matters identified.

- Materiality and tolerable misstatement thresholds used.

- Any indicators of possible management bias regarding accounting estimates and the application of accounting principles.

- Other matters that may be relevant to the primary government's audit, such as exceptions noted in the component's management representation letter.

- Audit results.

We reviewed the results of separately performed work and incorporated the results into the audit of the primary government, including the following, as applicable:

- Aggregation of misstatements. – We noted one uncorrected misstatement that led to cash and cash equivalents being understated by \$4,481,520, the misstatement is documented in [TeamMate file - S1WorkersCompensation Funds-FS24] we included this misstatement in the AOM here [[Aggregation of Misstatements \(GAAP\)](#)]. Other misstatements in the WCP audit were related to minor formatting issues, presentation errors in the notes to the financial statements and RSI. These will not impact the state ACFR.

- Significant difficulties or disagreements. - No issues noted.

- Reported amounts and disclosures audited in other work traced to the financial statements of the primary government. - No issues noted.

- Any potential fraud, noncompliance, abuse or other matters identified should be re-evaluated for the primary government. - No issues noted.

## State of Washington

Any report modifications, significant deficiencies or material weaknesses to the extent they are material to the primary government. - No issues noted.

We will **not** make reference to other SAO audits in our audit report.

### **State ACFR to Workers' Compensation ACFR Tie Out**

We performed the following procedures to tie the Workers' Compensation fund in the 2024 State ACFR to the audit Workers' Compensation Program Financial Statements:

We compared the balances in the WA State ACFR for the Workers' Compensation Fund to the Workers' Compensation Fund financial statements.

See the Workers' Compensation Fund FY24 audited report at: [FY24 WCP Audit Report](#)

See conclusions for each statement below:

Statement of Net Position [[FY24 WCP Tie Out](#)] **No issues noted.**

Statement of Revenue, Expenses and Changes in Net Position [[FY24 WCP Tie Out](#)] **No issues noted.**

Statement of Cash Flows [[FY24 WCP Tie Out](#)] **No issues noted.**