

IT Audit Central Projects

General

Code: C1-ITACentral-SP25
Name: IT Audit Central Projects
Group: IT Audit
Type:
Location:
Scope:

Team

Lead:
Manager: Karen Wilson

Procedures

B.5.PRG - DELETE

Procedure Step: Controls over EFTs
Prepared By: (None)
Reviewed By: (None)

Purpose/Conclusion.*

Purpose:

IT Audit Central Projects

To determine whether controls over Electronic File Transfer disbursements are adequate to safeguard public resources. [To determine if EFT disbursements are valid and supported by adequate documentation.]

Conclusion:

Testing Strategy:

The Public Request Exemption (RCW 42.56.420) protects some IT related information for cyber security purposes. The details documented in the record of work and support workpapers may qualify for this exemption. Auditors must include this statement in the workpapers: **"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".**

Electronic File Transfers (EFT) is a common method to pay vendors and employees quickly. Some transactions, such as payroll taxes, require electronic transfers. For this testing strategy's purpose Automated Clearing House (ACH) and Wire Type Transfers are considered "EFTs."

Contact SAOITAudit@sao.wa.gov for assistance or with questions regarding procedures described below.

The following procedures are **required**:

**Note: CAATs testing is optional for this step; however, because this information is not part of the initial data request received by the entities, the CAAT queries may take 2 - 4 weeks to obtain necessary information and develop queries. Auditors should evaluate, throughout the required steps, whether CAATs testing will be necessary and submit an [IT HelpDesk](#) as soon as possible.*

1. Obtain policies and determine if the elements similar to those outlined in BARS Manual [3.8.11](#) Electronic Funds Transfers (RCW 39.58.750) are included.
2. Consider what types of EFT transactions are performed:
 - Payments made via direct deposit, ACH, EFT or any other electronic payment method (i.e. payroll, taxes, benefits, vendor payments)
 - Online banking or bill pay
 - Transfers between entity bank accounts
 - Wire transfers
3. Determine which EFT transaction type(s) pose the highest risk for the entity's activity and organization. There have been increased focus on direct deposits and vendor payments by malicious actors.

IT Audit Central Projects

4. Gain an understanding (this may require talking to multiple departments such as payroll and accounts payable) of the following:

What are the procedures to add or change employee and/or vendor profiles including contact information and direct deposit bank accounts.

*If changes are not requested in-person, confirm how the department verifies the authenticity of new payee or change requests. Any request made through an employee portal system, phone call, email, instant message or physical form not delivered in-person, etc., should have a multi-factor authentication (MFA) or verification method. MFA or verification could be via virtual meeting. Email is not a suggested practice as malicious actors often obtain access to email accounts when conducting these types of fraud. Phone is adequate if there is some method of identifying you are talking to the correct person such as, confirming additional information only the original payee would know (i.e., providing the prior bank account number on file or details of their payment history is a common practice). Sending physical letters confirming the request was received, request was made, and if this request was not made by the vendor/employee they should contact the agency, is a form of verification; however standard mail generally takes too long and fraud could occur while in transit. As we would expect very few additions/changes to payee profile information, even at large governments, we would expect agencies to receive positive affirmations **before** making contact/bank changes or adding new EFT information in their system.*

Note: Previous guidance was to use existing contact information to conduct follow-up confirmations. Cyber actors are now requesting payee contact information to be changed (i.e., phone number, email and less often, mailing address) several months prior to requesting bank account changes. We, therefore, suggest the entity contact the payee based on existing contact information before **any** payee profile contact or banking changes (i.e., phone number, email, physical address, bank account information). Agencies should not use any contact information provided by the request but instead use existing information or by looking up the contact information (i.e., on-line, employee supervisor, person who is responsible for the purchases through a vendor, etc.)

Are changes to payee information logged in some method that is free from alteration?

This log should identify responsible parties and affected fields but not details such as old or new bank account numbers. These logs should be monitored for reasonableness (including volume of requests) and can be cross-referenced to any system audit reports that capture changes made to profiles.

Is there a dedicated, isolated, computer used specifically for EFT transactions to the bank? Is this computer free of all unnecessary software and not used for email, internet surfing, etc.?

IT Audit Central Projects

This increases security protection. If a dedicated, isolated computer is not used, identify the security protection controls established to provide assurance that bank account access is not compromised. Consider the volume and dollar amount of activities when evaluating this control.

Does the bank offer any automated controls regarding electronic transfers (i.e., emails)? Are these controls used by the entity?

This can increase the timeliness of identifying and correcting unexpected disbursements. Confirm entity reviews automated notification of EFT transactions (i.e., call-back, email, etc.) for reasonableness (i.e., for transactions that are routine, a transaction mid-cycle should be identified as a red-flag). Entities should have a documented risk assessment for any controls offered by the bank, but not utilized.

Who are the users with access and rights to initiate and process the EFTs?

Access should be limited to only those necessary to perform these duties and retain proper segregation of duties (i.e., the individual(s) responsible for initiating EFTs should not have access or responsibilities related to changing profiles, inputting payments, or reconciling bank accounts, etc.) Consider TeamMate testing strategy at Accountability | IT Controls | User Access for a more in-depth review and risks related to user access. If this segregation is not feasible, the entity should have documented risk assessment and compensating controls (consider reviewing and providing the Center's [Segregation of Duties: Essential Internal Controls](#)).

Is the documentation to support the legal and allowable purposes handled the same as non-EFT transactions?

Are there any outputs (reports or downloads) where the bank account number is in plain text? How does the agency limit the access to these outputs?

Do those who approve payments have access to all types of transactions?

Minutes or other reports should clearly show EFT and non-EFT payments. Auditors and management should be aware of report criteria to ensure completeness.

If the agency allows expenditures to be disbursed prior to approval, is there a method to collect EFTs that are not approved?

Are EFTs reconciled by batch or individual transaction?

Some banks process EFTs in a batch, especially for payroll. However, there should be a control to trace total bank batch to the individual transactions for full or partial reconciliation.

IT Audit Central Projects

Is there insurance, bank or other coverage for potential fraudulent claims? What are the terms to timely identify and notify the insurance company?

To receive coverage, many banking and insurances have a very tight turn around to detect and report a fraudulent EFT transaction. Entities should know their bank and/or insurance company's expectations and ensure bank statements that process EFTs are reconciled before those thresholds.

What is the corrective plan for fraudulent or erroneous transactions?

Agencies should have a documented plan or policy.

Did the government have any loss of money or data from EFT, or other incidents, since the last audit?

The government or audit team should report any loss of money or data through the SAO Fraud website. Security details should never be in email, a body of a helpdesk or the fraud reporting site. If the auditor or the entity has questions, please request a meeting with [IT Audit](#).

Consider the following procedures:

- Testing strategy available at [Accountability | IT Controls | User Access](#). This may include:
 - Access to online banking portal function
 - Ability to initiate the EFT transaction function
 - Access to text or excel files and folders that maintain batched EFT downloads
 - Access to application(s) bank account records
 - Ability to modify configuration rules of automated interfacing to the banking site function
- As EFT information is in electronic format (text or pdf), some potential CAATs may be requested and tested. These may include:
 - Compare routing / bank numbers used between system and bank
 - Payees with multiple bank account combinations
 - Payees using the same bank account information
 - Audit trail of changed banking information to payee profile

As these are not pre-populated CAAT queries, requests may take 2-4 weeks. Auditors should submit an [IT HelpDesk](#) as soon as possible.

IT Audit Central Projects

- Confirm entity's bank agreement regarding the verification to only permit transactions from specific authorized users.

Changes to staff with bank authorization should only be made by resolution of the governing body. Bank should have controls that reject transactions from any non-authorized users.

- Testing strategy available at [Accountability | IT Controls | Patch Management](#) for systems and/or computers used in the EFT process.
- Identify EFT disbursements from bank statement(s) and review supporting documentation for validity and adequate support.

In reviewing documentation, auditors should specifically verify the EFT bank account used and amount. This test may also be done as part of the general disbursement work.

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](#).
- Auditors must include this statement in the ROWD and 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:

AUDIT CRITERIA

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

BARS 3.8.11 Electronic Funds Transfers

RCW [39.58.750](#) Receipt, disbursement, or transfer of public funds by wire or other electronic communication means authorized

Record of Work Done:

IT Audit Central Projects

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

B.5.PRg - DELETE

Procedure Step: [Application System] - Understand Key Access Controls

Prepared By: (None)

Reviewed By: (None)

Purpose/Conclusion:

Purpose:

To gain an understanding of controls over access to [application system], identify key application system access controls, and assess whether the design of controls is capable of providing reasonable assurance that application system access is limited to only that necessary for staff to perform their duties.

Conclusion:

We gained an understanding of controls over access to [application system] and identified key application system access controls.

We also assessed the design of the controls, and determined it is [not] capable of providing reasonable assurance that application system access is limited to only that necessary for staff to perform their duties. [If exceptions were noted, link to related audit issue(s)]

Testing Strategy:

PUBLIC REQUEST EXEMPTION

The Public Request Exemption (RCW 42.56.420) protects some IT related information 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 the workpapers: **"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."**

IT Audit Central Projects

Gain an Understanding of Application System Access Controls

The auditor must gain an understanding of access controls over the application system. (Note: if access controls will be evaluated for multiple application systems, this step and the related testing step should be documented separately for each application system). The auditor's understanding should focus on key controls, which are the controls critical to providing reasonable assurance that access is limited to only that necessary for staff to perform their duties.

The agency needs to control access to its data. This is usually done by limiting access to the data through an application, which can also ensure programmed edits are run and that an audit trail is maintained to show who input or modified data. Limiting access to data through the application may be controlled by the operating system or third party software that will only let the application have access to the data. We normally break up our review of access control into three areas: application systems, data files, and program libraries.

Application system access considerations include:

- Identify who is the security administrator and who is the database administrator. Ideally, these should be different people.
- Consider how the agency grants access to staff.
 - Who initiates additions, deletions, and updates to user access?
 - How are requests for additions, deletions and updates to user access communicated to the Security Administrator? For example, does a supervisor authorize staff to have access to the application system?
 - How is access updated for terminated employees or employees whose job responsibilities have changed?
- How is the access controlled (within the application, operating system, or third party software)?
- Are hardened passwords enforced?
- Does the system have intruder lockout? If so, how many failed attempts are allowed before the system locks the user out?
- Does the system automatically log user off after a certain length of time and no activity?
- Is there logging of failed attempts?
- Are files containing logon IDs and passwords encrypted?
- Does the entity allow shared logon IDs?
- Does the entity allow the use of bogus IDs? (A bogus ID is an ID that does not identify the owner of the ID.)
- Can an individual be logged in to more than one computer at the same time?
- Do passwords expire? How often? Is a history maintained to prevent reusing the same passwords?

IT Audit Central Projects

- Are there any minimum requirements for passwords? For example, must be a certain length, contain upper and lower case letters, be a combination of letters/numbers/symbols, etc.

Additional considerations are included in the testing strategy at Accountability | IT Controls | User Access

Identify Key Access Controls

The auditor should document key application system access controls.

Assess Design of Key Access Controls

The auditor should assess the design of controls. If the auditor concludes the design of controls cannot achieve intended outcomes, the auditor must document an assessment of the control deficiency and report it appropriately. Typically, this would be considered a significant control deficiency (finding). The auditor may consider testing to assess the actual impact of identified design deficiencies.

If the auditor concludes the design of controls is capable of achieving intended outcomes, the auditor must assess the implementation and operating effectiveness of the key controls (performed in related Test Key Controls step).

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.

Understanding of [Application System] Access Controls:

[Document understanding. As part of the understanding, describe the sources of the information obtained (name/title of person interviewed, documents reviewed, dates of any observations, etc.)]

Identify Key Access Controls:

[List]

Assess Design of Key Access Controls:

We assessed the design of access controls over [application system] and determined it is [not] capable of providing reasonable assurance that access is limited to only that necessary for staff to perform their duties. We will test the implementation and effectiveness of identified key controls in a later step.

[Modify as necessary and summarize any exceptions. Auditors may consider testing to assess the actual impact of identified design deficiencies.]

IT Audit Central Projects

B.5.PRG - DELETE

Procedure Step: [Application System] - Test Key Access Controls

Prepared By: (None)

Reviewed By: (None)

Purpose/Conclusion:

This step is only applicable if auditors determined the design of controls is capable of providing reasonable assurance that access to the application system is limited to only that which is necessary for staff to perform their duties. Otherwise, an issue should be noted at the "design assessment" point and this step can be deleted.

Purpose:

To test key controls over access to [application system] and assess the implementation and operating effectiveness of those controls.

Conclusion:

We tested key access controls, and determined they had been implemented and were effective to provide reasonable assurance that access is limited to only that necessary for staff to perform their duties. [OR: describe results. If exceptions were noted, link to related audit issue(s).]

Testing Strategy:

PUBLIC REQUEST EXEMPTION

The Public Request Exemption (RCW 42.56.420) protects some IT related information 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 the workpapers: **"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".**

Control Testing

Auditors should list and test each key application system access control identified in the related "Understand Key Access Controls" step.

IT Audit Central Projects

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 by the test.

Control Assessment

Auditors should document their assessment of the implementation and operating effectiveness of key application system access controls, based on their testing.

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.

Application System Access Control Testing for [Key Control]:

[Document control testing for each key application system access control identified in the related Understand Key Controls step]

Application System Access Control Assessment:

Based on our testing, we determined key controls over access to [application system] had [not] been implemented. [Modify as necessary and summarize any exceptions]

We also determined controls were [not] effective to provide reasonable assurance that application system access is limited to only that necessary for staff to perform their duties. [Modify as necessary and summarize any exceptions]

B.5.PRГ - DELETE

Procedure Step: Understand Key Data File Access Controls

Prepared By: (None)

Reviewed By: (None)

IT Audit Central Projects

Purpose/Conclusion.

Purpose:

To gain an understanding of controls over access to data files, identify key data file access controls, and assess whether the design of controls is capable of providing reasonable assurance that data file access is limited to only that necessary for staff to perform their duties, and data files are protected from unauthorized modification or destruction.

Conclusion:

We gained an understanding of controls over access to data files and identified key data file access controls.

We also assessed the design of the controls, and determined it is **[not]** capable of providing reasonable assurance that data file access is limited to only that necessary for staff to perform their duties, and data files are protected from unauthorized modification or destruction. **[If exceptions were noted, link to related audit issue(s)]**

Testing Strategy.

PUBLIC REQUEST EXEMPTION

The Public Request Exemption (RCW 42.56.420) protects some IT related information 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 the workpapers: **"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".**

Gain an Understanding of Data File Access Controls

The auditor must gain an understanding of access controls over key data files. The auditor's understanding should focus on key controls, which are the controls critical to providing reasonable assurance that access is limited to only that necessary for staff to perform their duties, and that data files are protected from unauthorized modification or destruction.

The agency needs to control access to its data. This is usually done by limiting access to the data through an application, which can also ensure programmed edits are run and that an audit trail is maintained to show who input or modified data. Limiting access to data through the application may be controlled by the operating system or third party software that will only let the application have access to the data. We normally break up our review of access control into three areas: application systems, data files, and program libraries.

Data file access considerations include:

- Does the system only allow access to the data via the application?

IT Audit Central Projects

- Does the system log access attempts and if so, who reviews? Can the log be altered or deleted?
- Do programmers have access to the production data files?
- Is there a history file that provides for an adequate audit trail? This should show who performed the action, when the action occurred, and what information was entered/deleted. Who has access to the history file?

Identify Key Controls

The auditor should document key data file access controls.

Assess Design of Controls

The auditor should assess the design of controls. If the auditor concludes the design of controls cannot achieve intended outcomes, the auditor must document an assessment of the control deficiency and report it appropriately. Typically, this would be considered a significant control deficiency (finding). The auditor may consider testing to assess the actual impact of identified design deficiencies.

If the auditor concludes the design of controls is capable of achieving intended outcomes, the auditor must assess the implementation and operating effectiveness of the key controls (performed in related Test Key Controls step).

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.

Understanding of Data File Access Controls:

[Document understanding. As part of the understanding, describe the sources of the information obtained (name/title of person interviewed, documents reviewed, dates of any observations, etc.)]

Identify Key Controls:

[List]

Assess Design of Controls:

We assessed the design of access controls over data files and determined it is [not] capable of providing reasonable assurance that data file access is limited to only that necessary for staff to perform their duties, and that data files are protected from unauthorized modification or

IT Audit Central Projects

destruction. We will test the implementation and effectiveness of identified key controls in a later step. [Modify as necessary and summarize any exceptions. Auditors may consider testing to assess the actual impact of identified design deficiencies.]

B.5.PRG - DELETE

Procedure Step: Test Key Data File Access Controls

Prepared By: (None)

Reviewed By: (None)

Purpose/Conclusion:

This step is only applicable if auditors determined the design of controls was capable of providing reasonable assurance that access to data files is limited to only that necessary for staff to perform their duties, and that data files are protected from unauthorized modification or destruction. Otherwise, an issue should be noted at the “design assessment” point and this step can be deleted.

Purpose:

To test key controls over access to data files and assess the implementation and operating effectiveness of those controls.

Conclusion:

We tested key data file access controls, and determined they had been implemented and were effective to provide reasonable assurance that data file access is limited to only that necessary for staff to perform their duties, and that data files are protected from unauthorized modification or destruction. [**OR:** describe results. If exceptions were noted, link to related audit issue(s).]

Testing Strategy:

PUBLIC REQUEST EXEMPTION

The Public Request Exemption (RCW 42.56.420) protects some IT related information 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 the workpapers: **"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".**

IT Audit Central Projects

Control Testing

Auditors should list and test each key data file access control identified in the related "Understanding Key Controls" 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 by the test.

Control Assessment

Auditors should document their assessment of the implementation and operating effectiveness of key data file access controls, based on their testing.

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.

Data File Access Control Testing for [Key Control]:

[Document control testing for each key data file access control identified in the related Understanding Key Controls step]

Data File Access Control Assessment:

Based on our testing, we determined key controls over access to data files had [not] been implemented. [Modify as necessary and summarize any exceptions]

We also determined controls were [not] effective to provide reasonable assurance that data file access is limited to only that which is necessary for staff to perform their duties, and that data files are protected from unauthorized modification or destruction. [Modify as necessary and summarize any exceptions]

B.5.PR.G - DELETE

IT Audit Central Projects

Procedure Step: Understand Key Program Library Access Controls
Prepared By: (None)
Reviewed By: (None)

Purpose/Conclusion:

Purpose:

To gain an understanding of controls over access to program libraries, identify key program library access controls, and assess whether the design of controls is capable of providing reasonable assurance that program library access is limited to only that which is necessary for staff to perform their duties and data program libraries are protected from unauthorized modification or destruction.

Conclusion:

We gained an understanding of controls over access to program libraries and identified key program library access controls.

We also assessed the design of the controls, and determined it is [not] capable of providing reasonable assurance that program library access is limited to only that necessary for staff to perform their duties, and data program libraries are protected from unauthorized modification or destruction. [If exceptions were noted, link to related audit issue(s)]

Testing Strategy:

PUBLIC REQUEST EXEMPTION

The Public Request Exemption (RCW 42.56.420) protects some IT related information 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 the workpapers: **"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".**

Gain an Understanding of Program Library Access Controls

The auditor must gain an understanding of access controls over program libraries. The auditor's understanding should focus on key controls, which are the controls critical to providing reasonable assurance that access is limited to only that necessary for staff to perform their duties, and data program libraries are protected from unauthorized modification or destruction.

The agency needs to control access to its data. This is usually done by limiting access to the data through an application, which can also ensure

IT Audit Central Projects

programmed edits are run and that an audit trail is maintained to show who input or modified data. Limiting access to data through the application may be controlled by the operating system or third party software that will only let the application have access to the data. We normally break up our review of access control into three areas: application systems, data files, and program libraries.

Program library access considerations include:

- Does the system log access attempts and if so, who reviews?
- Are test environments that are network attached secured as they are in the production environment?
- Is access controlled so that only approved changes to programs can be placed into production?
- Do programmers have access to the production programs?

Identify Key Controls

The auditor should document key program library access controls.

Assess Design of Controls

The auditor should assess the design of controls. If the auditor concludes the design of controls cannot achieve intended outcomes, the auditor must document an assessment of the control deficiency and report it appropriately. Typically, this would be considered a significant control deficiency (finding). The auditor may consider testing to assess the actual impact of identified design deficiencies.

If the auditor concludes the design of controls is capable of achieving intended outcomes, the auditor must assess the implementation and operating effectiveness of the key controls (performed in related Test Key Controls step).

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.

Understanding of Program Library Access Controls:

[Document understanding. As part of the understanding, describe the sources of the information obtained (name/title of person interviewed, documents reviewed, dates of any observations, etc.)]

Identify Key Controls:

[List]

IT Audit Central Projects

Assess Design of Controls:

We assessed the design of access controls over program libraries and determined it is [**not**] capable of providing reasonable assurance that program library access is limited to only that necessary for staff to perform their duties, and that program libraries are protected from unauthorized modification or destruction. We will test the implementation and effectiveness of identified key controls in a later step. [Modify as necessary and summarize any exceptions. Auditors may consider testing to assess the actual impact of identified design deficiencies.]

B.5.PRГ - DELETE

Procedure Step: Test Key Program Library Access Controls

Prepared By: (None)

Reviewed By: (None)

Purpose/Conclusion:

This step is only applicable if auditors determined the design of controls is capable of providing reasonable assurance that access to program libraries is limited to only that necessary for staff to perform their duties, and that program libraries are protected from unauthorized modification or destruction. Otherwise, an issue should be noted at the "design assessment" point and this step can be deleted.

Purpose:

To test key controls over access to program libraries and assess the implementation and operating effectiveness of those controls.

Conclusion:

We tested key program library access controls, and determined they had been implemented and were effective to provide reasonable assurance that program library access is limited to only that necessary for staff to perform their duties, and that program libraries are protected from unauthorized modification or destruction. [**OR: describe results. If exceptions were noted, link to related audit issue(s).**]

Testing Strategy:

PUBLIC REQUEST EXEMPTION

The Public Request Exemption (RCW 42.56.420) protects some IT related information for cyber security purposes. The details documented in the

IT Audit Central Projects

record of work and supporting workpapers may qualify for this exemption. Auditors must include this statement in the workpapers: **"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"**.

Control Testing

Auditors should list and test each key program library access control identified in the related "Understand Key Controls" 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 by the test.

Control Assessment

Auditors should document their assessment of the implementation and operating effectiveness of key program library access controls, based on their testing.

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.

Program Library Access Control Testing for [Key Control]:

[Document control testing for each key program library access control identified in the related Understand Key Controls step]

Program Library Access Control Assessment:

Based on our testing, we determined key controls over access to program libraries had [**not**] been implemented. [Modify as necessary and summarize any exceptions]

We also determined controls were [**not**] effective to provide reasonable assurance that program library access is limited to only that necessary for staff to perform their duties, and that program libraries are protected from unauthorized modification or destruction. [Modify as necessary and summarize any exceptions]

IT Audit Central Projects

B.5.PRG - DELETE

Procedure Step: Test User Access

Prepared By: (None)

Reviewed By: (None)

Purpose/Conclusion:

Purpose:

To determine whether access granted to user screens, data files, and production libraries was appropriate.

Conclusion:

We determined access granted to user screens, data files, and production libraries was **[not]** appropriate. **[If exceptions were noted, link to related audit issue(s)]**

Testing Strategy:

PUBLIC REQUEST EXEMPTION

The Public Request Exemption (RCW 42.56.420) protects some IT related information 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 the workpapers: **"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"**.

Auditors should request a report showing access to the user screens, data files, and production libraries (programs) so they can evaluate access to these areas. Depending on the size of the agency and the number of screens and data files, doing this for all employees for all user screens and data files may be too much. If so, auditors can limit the scope to just the critical screens and data files.

Consider using reports or requesting queries to identify potential high-risk users, such as:

- Any user that may have more rights than needed to perform their typical job duties.
- Current, or former, employees who may still have rights to previous job assignment's functions.
- Employees with rights to initiate and electronically approve or post transactions.

IT Audit Central Projects

- Users able to add or change user accounts or software application settings.
- Users with the ability to add or change employees, vendors, or customers' master files.
- Users with the ability to maintain master tables that affect software calculations.
- Generic authentication IDs that can post transactions. (e.g., substitutes taking enrollment.)
- External users.

Remember, for the most part, we are only concerned with those individuals that have UPDATE access. Read access is not as critical, depending on if there is sensitive data which individuals should not be able to view. A data file containing Logon IDs with passwords (unless encrypted) is an excellent example of read access being inappropriate! Even if encrypted, read access to this file should probably be limited to security administrators.

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.

Access Types Selected for Testing:

[List]

Testing for [Access Type]:

[Describe testing for each selected access type]

Summary of Results:

We determined access granted to user screens, data files, and production libraries was [not] appropriate. [Modify as necessary and summarize any exceptions]

B.5.PRg - DELETE

IT Audit Central Projects

Procedure Step: Summary and Conclusion - Electronic Access

Prepared By: (None)

Reviewed By: (None)

Purpose/Conclusion.*

Purpose:

To evaluate electronic access controls as a whole and the sufficiency and appropriateness of evidence based on the results of our testing.

Conclusion:

Based on our evaluation, we determined controls were [**not**] properly designed, implemented, and effective overall to provide reasonable assurance that:

- Electronic access is only granted to the extent necessary for staff to perform their duties
- Data files and program libraries are protected from unauthorized modification or destruction.

[**OR: Modify as necessary and summarize any new or overall conclusions about exceptions with links to related audit issue(s).**]

We also determined that evidence obtained was sufficient and appropriate to provide a reasonable basis for conclusions on controls.

Testing Strategy.*

To supplement the individual evaluations and conclusions on electronic access controls, auditors are also required to evaluate and conclude on electronic access controls in aggregate.

In making this evaluation, auditors should specifically consider:

- *How any access control deficiencies may affect other access controls.*
- *Whether the potential errors that may result from deficiencies might be either prevented or detected and corrected by other controls.*
- *The nature, likelihood and magnitude of actual and potential errors resulting from control deficiencies.*

Auditors should also consider the sufficiency and appropriateness of evidence in relation to the understanding and testing of electronic access controls as a whole. If additional procedures are needed based on this evaluation, they can be either documented in this step or documented elsewhere and referenced here.

IT Audit Central Projects

In making this evaluation, auditors should specifically consider:

- *Whether the evidence obtained is relevant, valid, and reliable*
- *Whether enough appropriate evidence exists to address the audit objectives and support the findings and conclusions to the extent that would persuade a knowledgeable person that the findings are reasonable*
- *Whether auditors used information provided by officials of the audited entity as part of their evidence. If so, they should determine what the officials of the audited entity or other auditors did to obtain assurance over the reliability of the information*
- *Whether testimonial evidence is objective, credible, and reliable*
- *Whether there are any significant uncertainties or limitations with tests or evidence, and the effect of these on our audit and report.*
- *Whether there is a need for more procedures or evidence to determine whether control deficiencies resulted in actual errors during the period, or to determine the nature and extent of actual effects of weaknesses or to improve the precision of estimates.*
- *Whether controls changed during the course of the audit period and whether sufficient appropriate evidence was obtained for the entire period.*
- *Whether further procedures or evidence is needed to assess potential mitigating controls or entity actions to follow up on weaknesses or actual errors.*
- *Whether the audit encountered a different level or type of risk than tests were designed to detect.*
- *Whether changes to the audit plan are needed.*

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.

Overall Evaluation of Electronic Access Controls:

We considered the results and conclusions from our understanding and testing of electronic access controls both individually and in aggregate to determine effectiveness of controls as a whole.

[If no deficiencies were noted: We noted no individual control deficiencies, and no further deficiencies were identified when considering the design, implementation and effectiveness of controls as a whole.]

[If deficiencies were noted: List each individual deficiency and conclude on whether it is mitigated, unaffected or amplified by the overall design, implementation and effectiveness of electronic access controls. If mitigated, then describe the mitigating controls, their effect and any related

IT Audit Central Projects

evidence or design logic. If amplified, then describe the design logic or evidence leading to this conclusion. Conclude on the significance of identified control deficiencies.]

Overall Evaluation of Evidence:

We considered audit procedures and evidence obtained and determined that no further work was necessary to support our control conclusions.

[**OR:** Modify as necessary to describe follow-up work or to include rationale or approach to significant uncertainties or limitations]