Office of the Washington State Auditor
Pat McCarthy

Performance Audit

Contract Assurances for Vendor-Hosted State Information Technology Applications

December 13, 2018

Report Number: 1022707

Table of Contents

State Auditor's Office contacts

State Auditor Pat McCarthy
360-902-0360, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance Audit
360-902-0376, Scott.Frank@sao.wa.gov

Erin Laska – Principal Performance Auditor
360-778-2697, Erin.Laska@sao.wa.gov

Olha Bilobran – Senior Performance Auditor
360-725-5606, Olha.Bilobran@sao.wa.gov

Will Clark – Performance Auditor
360-725-5632, William.Clark@sao.wa.gov

Isaiah Berg – Performance Auditor
360-725-5619, Isaiah.Berg@sao.wa.gov

Hannah Febach – Performance Auditor
360-725-5356, Hannah.Febach@sao.wa.gov

Kathleen Cooper – Director of Communications
360-902-0470, Kathleen.Cooper@sao.wa.gov

To request public records

Public Records Officer
360-725-5617, PublicRecords@sao.wa.gov

Executive Summary

Background

State agencies increasingly rely on vendors to provide information technology (IT) services and operate systems critical to state agencies and the public. These IT vendors often host systems that process and store confidential state data off-site or in the cloud, where the state has little or no direct control over the security of its data. However, agencies are ultimately responsible for the state's data, even when it is managed and hosted in vendor applications.

Because of the growing risks related to state IT assets, including those managed by private vendors, our Office chose to conduct a performance audit of IT contract assurances for vendor-hosted IT applications. The audit focused on how state agencies ensure their IT vendors safeguard those applications and the data they hold. Specifically, the audit looked at whether state agencies include appropriate language in their contracts with IT vendors requiring them to comply with state and agency IT security requirements. The audit also assessed whether state agencies are using leading practices when monitoring their IT vendors, and it reports on the assurances agencies include in contracts to protect the state in the event of a security incident or data breach.

Have selected IT contracts included appropriate provisions to address the state's IT security requirements?

State policy requires a vendor to meet both the state's general IT security standards and agency's specific standards to protect the state's information. However, state IT security standards do not specify how agencies should verify vendor compliance with those standards. Most of the reviewed contracts required vendors to comply with the state's general IT security standards, but only one included the agency's specific standards. Moreover, two contracts did not require vendor compliance with state or agency IT security requirements. In addition, the IT applications associated with three of the seven contracts did not go through an Office of Cyber Security (OCS) security design review, required under certain conditions, to ensure compliance with the state's security standards.

Do selected state agencies follow leading practices to ensure vendors comply with the IT security requirements in their contracts?

Leading practices suggest agencies should monitor their contractors on an ongoing basis to ensure they comply with IT security requirements. The agencies included in this audit could improve their monitoring practices by more consistently following these leading practices. We found agencies did not use risk assessment results to develop specific contractual monitoring requirements. In addition, agencies did not specify how vendors can demonstrate compliance with contractual IT security requirements, and only two of the five agencies actively monitored their vendors' compliance with most contractual security requirements. Likewise, although most agencies required vendors to adhere to the state's IT standards, none of the agencies verified compliance in accordance with contractual provisions. Also, several agencies could do more to specify roles and responsibilities, and to communicate regularly with vendors about IT security.

This report does not identify individual agencies or applications

IT security information is exempt from public disclosure in accordance with RCW 42.56.420(4). To protect the IT security of our state, this report does not include the names of the selected agencies, names of the IT applications we reviewed nor any detailed descriptions of our findings. Disclosure of such detail could potentially be used by a malicious attacker against the state. Detailed findings and recommendations were provided to each agency we reviewed and the Governor's Office.

The state's Office of the Chief Information Officer (OCIO) and the Office of Cyber Security (OCS) are housed within Washington Technology Solutions (WaTech), which is state agencies' partner in IT security.

Finally, the Department of Enterprise Services (DES) could help agencies manage IT contracts more effectively by including specific IT guidance in its policies and procedures for contracting.

What contractual provisions have selected state agencies included in vendor contracts to protect the state in case of a data breach?

Indemnification clauses, notification clauses and cyber-liability insurance are good tools to protect the state, but there are no agreed-upon standards for these. All seven contracts included indemnification language to protect the state in the event of a data breach, but the language could be improved for some contracts while one contract had especially good language. The state's Office of the Chief Information Officer (OCIO) has some good indemnification language agencies can use, but agencies have to request it. Additionally, the required timelines for notifying the state of a data breach in most contracts were longer than the state's security policies would suggest. Finally, we noted one contract required cyber-liability insurance, and two other vendors carry the insurance.

State Auditor's Conclusions

When state agencies contract with IT vendors, the agencies can save the resources they would otherwise need to develop applications themselves. However, when agencies outsource IT applications, they must take reasonable steps to ensure their vendors treat the public's data with the appropriate level of care.

That is where the contracts for services become important. The legal contracts between agencies and their vendors should include appropriate provisions to protect the public's information. As this audit shows, most state agencies use contract management practices that fall short of what is needed in the cybersecurity realm. The agencies we reviewed did not conduct the types of formal risk assessments that are needed to identify appropriate security provisions to include in their contracts; nor did they consistently use the provisions that were in the contracts to monitor vendor performance.

While state agencies are ultimately responsible for the security of the data they outsource to vendors, they need better support in the form of clear guidance, standards and draft language to use in their contracts. The OCIO and DES should develop draft language about several important elements that should be included in every IT contract. These elements could include defining "security breach," setting notification expectations, and specifying how a vendor will compensate the public if something goes wrong.

Finally, the OCIO should clarify the state IT security standards and provide more guidance to the state agencies to help ensure they include compliance requirements with appropriate state IT security standards in their contracts. Additionally, the OCIO should examine alternatives to its current requirement that vendors meet the state's IT security standards. Vendors and agencies view some of the state's security guidelines as either too broad or too prescriptive. One solution would be to accept vendors that can demonstrate compliance with nationally recognized IT security frameworks or federal IT security standards instead.

Recommendations

We made a series of recommendations to DES to improve the guidance it provides to state agencies that contract for IT services. We also made recommendations to OCIO to provide more guidance and clarity in how agencies and their vendors should comply with state standards to ensure the security of confidential data in vendor-hosted applications. Finally, we made a series of recommendations to state agencies to help them comply with state law and follow best practices as they develop their contracts and monitor vendor performance.

Next steps

Our performance audits of state programs and services are reviewed by the Joint Legislative Audit and Review Committee (JLARC) and/or by other legislative committees whose members wish to consider findings and recommendations on specific topics. Representatives of the State Auditor's Office will review this audit with JLARC's Initiative 900 Subcommittee in Olympia. The public will have the opportunity to comment at this hearing. Please check the JLARC website for the exact date, time, and location (**www.leg.wa.gov/JLARC**). The State Auditor's Office conducts periodic follow-up evaluations to assess the status of recommendations and may conduct follow-up audits at its discretion. See **Appendix A**, which addresses the I-900 areas covered in the audit. **Appendix B** contains information about our methodology.

Background

State government is entrusted with vast amounts of confidential information so it can provide critical services, such as public safety, health and education to Washington residents. Examples of confidential information collected include social security numbers, health care information and arrest records.

Washington agencies are responsible for ensuring security over this data, whether they use applications they have developed and manage themselves or use applications developed and hosted by third-party vendors. Protecting the security of computer applications and the state's data they process is vital to maintain public confidence, to protect the public and to help ensure the continuity of government operations.

State agencies frequently contract with outside vendors for IT services

By contracting with IT vendors, agencies can save the resources otherwise needed to develop an application or to purchase the infrastructure needed to host and manage applications. When agencies use vendor-hosted applications, the vendor manages the application's hardware and software with minimal involvement of the state agency customer, which means that the state relinquishes direct control over security of the application and the confidential data it may contain.

Outsourcing IT applications is on the rise nationwide. According to the National Association of State Chief Information Officers' 2016 survey, four out of five states outsource at least some IT applications and services, a significant increase from 2010, when fewer than half did.

When agencies contract for IT services, they have to meet the state's contracting and IT policies

Agencies are required to ensure that third-party vendors and the applications they manage are held to the same IT security standards as agencies. Although state agencies are ultimately responsible for ensuring their vendors use appropriate security measures to protect IT applications and the state's data, strategic partners can help them during contract development and monitoring.

Two of these partners, the Department of Enterprise Services (DES) and the Office of the Chief Information Officer (OCIO) have the authority to write the policies, standards and guidelines related to IT security contracts that individual agencies must follow when procuring IT services.

DES sets the state's contracting policies

DES establishes overall state policies, standards and procedures for the procurement of goods and services by all state agencies. It is also responsible for establishing procurement processes for IT goods and services, using technology standards and policies established by OCIO.

DES is required by state law to develop contract monitoring policies and procedures to help all state agencies manage their contracts efficiently and effectively. It is also required to provide expertise and training on leading practices for state procurement.

DES can provide additional assistance and advice to state agencies if asked, but agencies are not required to consult DES if procurements are within their delegated authority.

The OCIO sets the state's IT standards and policies

State law requires state agencies to adhere to the OCIO's policies and standards. OCIO standards and policies govern the security, acquisition and confidentiality of computerized data at state agencies. The state's IT security standards, set out in Policy 141.10, apply to all IT activities, whether they are operated by an agency or on its behalf by a vendor. Specifically, Policy 141.10 requires agencies to ensure contracted vendors managing applications that process and store state data are held to the same IT security standards as the agencies themselves, including complying with the relevant state IT security standards and the agencies' IT security internal policies and procedures.

The state IT security standards are considered the minimum requirement, and many elements are intentionally broad to accommodate the IT environments present in different state agencies. Agencies must also develop their own IT security policies and procedures within the state IT security framework, and are encouraged to exceed the minimum requirements based on the risk to the data and complexity of the IT environment.

This audit examines whether state agencies are protecting the state's information when they outsource IT services

To help ensure that vendors managing applications for the state are protecting the state's confidential information from a security incident or breach, this performance audit assessed whether:

1. Selected IT contracts have included appropriate provisions to address the state's IT security requirements.
2. Selected state agencies follow leading practices to ensure vendors comply with the IT security requirements in their contracts.

Even with good IT security in place, incidents and breaches can still happen. To assess whether the state is protected in the event of a security breach the audit also examined:

3. What contractual provisions selected state agencies have included in vendor contracts to protect the state in case of a data breach.

Audit Results

Have selected IT contracts included appropriate provisions to address the state's IT security requirements?

Answer in brief

State policy requires a vendor to meet both the state's general IT security standards and agency's specific standards to protect the state's information. However, state IT security standards do not specify how agencies should verify vendor compliance with those standards. Most of the reviewed contracts required vendors to comply with the state's general IT security standards, but only one included the agency's specific standards. Moreover, two contracts did not require vendor compliance with state or agency IT security requirements. In addition, the IT applications associated with three of the seven contracts did not go through a security design review conducted by the Office of CyberSecurity (OCS), required under certain conditions, to ensure compliance with the state's security standards.

State policy requires a vendor to meet both the state's general IT security standards and agency's specific standards to protect the state's information

The Office of the Chief Information Officer (OCIO) established state policy 141.10, the state's IT security standards, to set requirements for maintaining system and network security, data integrity and confidentiality. The standards apply to all IT activities, whether they are operated by or for an agency, and represent the minimum IT security requirements for state agencies and their vendors.

OCIO security standards require agencies to include appropriate language in vendor contracts to require the vendor to comply with both the state IT security standards *and* the agency's own IT security policies. Because agencies' specific controls address their unique risks and IT environment, only requiring vendor compliance with the state's IT security standards may not be enough.

Specifically, OCIO security standards also state that agencies should identify the standards and controls that are appropriate to include in the contracts based on a formal IT risk assessment (OCIO 141.10 1.5(4)). Thus, agencies might require vendor's compliance with some but not all IT security standards. Contractor compliance with state standards may be demonstrated by mapping comparable vendor controls to the state standards, and adding supplemental controls to close gaps between the two (OCIO 141.10 1.5(5)). In addition, OCIO security standards state that agencies must request a security design review from OCS for an agency project impacting state IT assets outside the agency (OCIO 141.10 1.2.1 section 1(3)).

State IT security standards do not specify how agencies should verify vendor compliance

Though the state IT security standards require vendor compliance with the standards and appropriate language to be included in the contracts, OCIO policies do not specify how agencies should verify the vendor complied with these standards. Specifically, the state's IT security standards require state agencies to complete an independent audit every three years to confirm compliance with the standards. However, the standards are not clear as to whether vendor-hosted applications should be included as part of these audits (OCIO 141.10 1.6(1)).

Most of the reviewed contracts required vendors to comply with the state's general IT security standards, but only one included the agency's specific standards

We reviewed seven contracts at five agencies to assess whether the security requirements were included in the contract

Using the results from our 2015 state IT risk assessment and input from subject matter specialists, we selected five agencies with contracts for seven applications that are vendor-hosted, critical to the mission of the agency and contain confidential state information. When selecting contracts for review, we did not consider other factors, such as risk or monetary value of the contract. Because we did not complete an exhaustive search to identify all mission-critical, vendor-hosted, state applications with confidential state information, or used a random sample to choose agency contracts for this audit, these results cannot be generalized to all state agencies and IT vendor contracts. Nonetheless, the results provide insight into the issues all agencies likely face when they contract for IT services.

Exhibit 1 summarizes which contracts met this OCIO security policy requirement.

Exhibit 1 – State and agency IT security requirements in the contracts

Five agencies (A – E), with seven contracts (1 – 7) in total

	Agency letter / contract number							Number of contracts complying
Requirement	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**	
State IT security compliance requirement included	✓*	✓	×	✓	✓	×	✓	5/7
Agency IT security compliance requirement included	✓	×	×	×	×	×	×	1/7

✓ *means the contract* ***included*** *the requirement.*

× *means the contract* ***did not include*** *the requirement.*

**General statement requiring compliance with all state laws and regulations.*

Five of the seven contracts included provisions requiring the vendor to comply with the state's general IT security standards

For four contracts, the requirement that the vendor comply with the state's IT security standards is very specific, either by referencing the state IT security standards or by including a copy of the standards in their entirety. In addition, a fifth contract included a general statement requiring compliance with all state laws and regulations, but it could have been clearer by making a specific reference to the state IT security standards.

Only one contract included provisions addressing the agency's specific IT security standards

The audit found only one contract required the vendor to comply with the agency's own IT security requirements. The agency included this requirement as a performance measure in the contract and also required the vendor to comply with any future changes to the agency IT security policy.

None of the remaining contracts required vendor compliance with the agency's IT security requirements. Two agencies said that their agency IT security policies were based on OCIO 141.10 and not materially different from the state's standards, and officials saw no need to include this additional requirement in the contract. One agency reported it initially included provisions requiring compliance with agency IT security standards, but agreed to remove them during the negotiation process with the vendor. The final agency reported it was in the process of developing its own IT security policies, and plans to require vendors to comply with them after they are fully developed.

Two contracts did not require vendor compliance with state or agency IT security requirements

Both contracts included IT security safeguards which provided some level of assurance to the agencies. However, the agencies were not able to demonstrate how these safeguards align to either the state or agency IT security requirements as directed by state IT security standards.

The two contracts that did not require compliance with either state or agency IT security requirements, did not include the specific language because:

- One agency removed the language during contract negotiations when the vendor would not agree to comply with state IT standards. The vendor said it had already committed significant resources to achieving national IT security certifications, and would not undertake additional work to meet other standards requested by any one client.
- The second agency said such contract language was not an agency practice when the contract was signed in 2014, although it was a state requirement at that time. The agency has included a requirement to comply with state standards in subsequent contracts, but did not address the agency-specific language.

IT applications associated with three of the seven contracts did not go through an OCS security design review, required under certain conditions, to ensure compliance with the state's IT security standards

OCIO policy requires agencies to submit their IT projects for a security design review when the IT project meets certain criteria, such as agency IT projects that require significant IT investments, affect state IT assets outside the agency or are under OCIO oversight (OCIO 141.10 1.2.1 section 1(3)). OCS conducts the security design reviews. The purpose of this review is to determine whether the project complies with all state IT security standards before the system is implemented, providing assurance to the OCIO and the agency contracting for the vendor-hosted application.

The audit found three of the seven applications did not go through the design review. In the first case, agency staff agreed that the IT application should have gone through a security design review, but reported the agency did not submit the application for the review due to the proprietary nature of the vendor's IT security information. According to the OCIO, staff conducting design reviews frequently sign confidentiality agreements in such cases. In the second case, staff reported finalizing the contract with the vendor before the review could be conducted.

For the third application that did not go through the security design review, agency staff said their analysis determined the application did not require a review as defined in the state IT security standards. Determining if an application should receive a security design review was outside the scope of this audit.

Vendor-hosted applications that are required to, but do not receive, a security design review with OCS miss an opportunity to ensure the vendor-hosted applications are in compliance with state IT security standards before the contracts are signed and the applications are implemented. In addition to noncompliance with state policy, agencies have less assurance that mission-critical applications processing and storing confidential state data are secure.

Do selected state agencies follow leading practices to ensure vendors comply with the IT security requirements in their contracts?

Answer in brief

Leading practices suggest agencies should monitor their contractors on an ongoing basis to ensure they comply with IT security requirements. The agencies included in this audit could improve their monitoring practices by more consistently following these leading practices. We found agencies did not use risk assessment results to develop specific contractual monitoring requirements. In addition, agencies did not specify how vendors can demonstrate compliance with contractual IT security requirements and only two of the five agencies actively monitored their vendors' compliance with most contractual security requirements. Likewise, although most agencies required vendors to adhere to the state's IT standards, none of the agencies verified compliance in accordance with contractual provisions. Also, several agencies could do more to specify roles and responsibilities, and to communicate regularly with vendors about IT security. Finally, DES could help agencies manage IT contracts more effectively by including specific IT guidance in its policies and procedures for contracting.

Leading practices suggest agencies monitor their contractors on an ongoing basis to ensure they comply with IT security requirements

IT security contract monitoring relies on many of the same leading practices as general contract monitoring. However, IT procurements often require highly technical knowledge from agency specialists and vendors, and can be very complex. Cybersecurity is constantly evolving, influenced by rapidly changing security conditions, and therefore the agencies' monitoring efforts for IT security must also continuously adapt to reflect these changes.

DES is currently developing uniform policies and procedures to help agencies manage contracts, but during the audit and at the time of publication, there is no formal policy for agencies. To assess agency contract monitoring performance, this audit applied leading practices from:

- The *Global Technology Audit Guide (GTAG): Information Technology Outsourcing*, a widely recognized guide developed by an International Professional Association of Internal Auditors
- The *Project Management Body of Knowledge (PMBOK) Guide*, a set of widely accepted global standards that provide guidelines and rules for project and program management
- DES general contract management training materials

According to these leading practices, agencies should monitor and evaluate their contracts on an ongoing basis throughout the life of the contract to ensure vendor compliance with terms and conditions of the contract. In brief, agencies should:

- Conduct a risk assessment, and use its results to develop contractual requirements that facilitate monitoring
- Monitor and assess the vendor's performance against the contractual requirements
- Establish clear communication protocols in the contract that articulate the roles and responsibilities of the parties, project managers in particular, as well as how these parties will communicate

Appendix C offers more details about leading practices, the audit criteria and a related logic model. State policymakers could use these practices to enhance their IT and contracting guidance for agencies, and which agencies could use as a reference when renegotiating or developing new contracts with IT vendors.

Agencies could improve their monitoring practices by more consistently following the leading practices

To evaluate efforts of the five selected agencies in monitoring their seven contracts, we reviewed agencies' monitoring practices and processes. We then compared them to the leading practices listed in the previous section. We summarized the results of our comparisons in **Exhibit 2**. Each area of leading practices and how agencies' processes correspond to them are discussed further in the next several sections of the report.

Exhibit 2 – State agencies' IT security monitoring efforts

Five agencies (A – E), with seven contracts (1 – 7) in total

	Agency letter / contract number						
Requirement	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**
Risk assessment to identify appropriate IT security monitoring requirements conducted	×	×	×	×	×	×	×
IT security monitoring requirements included in the contract	✓	✓	×	✓	✓	✓	✓
How to demonstrate compliance specified	Partially	✓	×	✓	×	×	✓
Vendor IT security performance assessed by agency according to monitoring requirements in the contract	✓	✓	×	Ad hoc	×	×	Partially
Managers' roles and responsibilities included in the contract	✓	✓	×	✓	×	×	✓
IT *staff* roles and responsibilities included in other documents	✓	✓	×	×	×	×	✓
Clear communication protocols established	✓	✓	×	✓	×	×	✓

✓ *means the contract* ***included*** *the requirement.*
× *means the contract* ***did not include*** *the requirement.*

Agencies did not use risk assessment results to develop specific contractual monitoring requirements

The leading practices state that agencies should base their monitoring requirements on a formal risk assessment. Conducting a risk assessment and considering its results during contract development provides agencies and vendors with a better understanding of the risks and vendor compliance requirements to mitigate these risks.

As shown in **Exhibit 2a**, agencies did not conduct a formal risk assessment to identify threats, vulnerabilities and mitigating controls, and use those results to develop contractual IT security monitoring requirements.

Exhibit 2a – State agencies' IT security monitoring efforts

	Agency letter / contract number						
Requirement	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**
Risk assessment to identify appropriate IT security monitoring requirements conducted	×	×	×	×	×	×	×

× *means the contract* ***did not include*** *the requirement.*

The audited agencies used various other tools to assess risks when developing contracts or after the contracts were signed to gain assurance over vendor IT security. For example, one agency toured its vendor's facility; most conducted OCS security design reviews or used IT security checklists. One agency developed a thorough and detailed risk assessment tool to consider risks based on the category of data and hosting solution. However, none of the agencies developed detailed IT security monitoring requirements based on those risk assessment efforts.

When asked why they did not conduct a formal risk assessment to develop monitoring requirements, reasons varied. Some agencies said it was not required of them when the contract was developed, or the contract was signed before the agency had a chance to conduct the risk assessment, or agency staff lacked clear guidance on what a risk assessment should include.

When agencies do not conduct formal risk assessments and use the assessment results to develop their contract language, including requiring specific IT security controls and establishing criteria for monitoring vendors, the agencies risk signing contracts with unnecessary requirements that could increase the project costs. At the same time, some actual risks might go unidentified or not be mitigated by appropriate controls. As a result, contracts might not include requirements to comply with appropriate IT-security controls, or IT-security monitoring requirements might not be clearly detailed or required by the contract. In either case, staff may not be able to adequately monitor their contracts for key controls. In addition, newer staff responsible for contract monitoring might not be aware of the risks discussed and identified before the contract was signed and therefore might not monitor adequately. Moreover, conducting a formal risk assessment during contract development better prepares agencies for contract negotiations, by making clear where they can, and cannot, make concessions.

Agencies did not specify how vendors can demonstrate compliance with contractual IT security requirements

Agencies included IT-security monitoring requirements in six out of seven contracts (shown in **Exhibit 2b**). However, three of the contracts did not specify how the vendor would meet the requirements, including whether the monitoring could be done through regular audits or reviews, and which party would conduct the reviews. For example, one agency required the vendor to make its internal practices, books and records, available to determine compliance with Health Insurance Portability and Accountability Act (HIPAA) rules, but did not specify how frequently the compliance should be demonstrated and how the results should be provided to the agency. Additionally, five contracts required the vendor to comply with state IT security standards, but three of them did not specify how the vendor would demonstrate their compliance or how often.

Exhibit 2b – State agencies' IT security monitoring efforts

	Agency letter / contract number						
Requirements	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**
Monitoring requirements included in the contract	✓	✓	×	✓	✓	✓	✓
How to demonstrate compliance specified	Partially	✓	×	✓	×	×	✓

*✓ means the contract **included** the requirement.*
*× means the contract **did not include** the requirement.*

Only two of the five agencies actively monitored their vendor's compliance with most contractual security requirements

Leading practices state that agencies should use the monitoring criteria in their contracts to assess their vendor's performance. When agencies have an understanding of their vendor's IT security performance, they can more fully gauge the safety of state data and continuity of state operations.

The audit found only two of the five agencies acquired evidence of most of their contractual monitoring requirements, allowing them to actively monitor and assess the IT security performance of their contracted services (see **Exhibit 2c**). The monitoring included review of security scans, progress reports from the vendor, project management plans, compliance audits and update meetings.

Exhibit 2c – State agencies' IT security monitoring efforts

	Agency letter / contract number						
Requirement	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**
Vendor IT security performance assessed by agency according to monitoring requirements in the contract	✓	✓	×	Ad-hoc	×	×	Partially

✓ *means the contract* ***included*** *the requirement.*
× *means the contract* ***did not include*** *the requirement.*

However, the other three agencies which managed five of the contracts either did not have contract-specified tools to monitor their vendor, or did not use most of the tools identified in their contracts. For example, one agency contract allowed the agency to conduct an annual OCIO compliance audit of its vendor, but the agency has never used this tool to verify vendor's compliance with the contractual requirement.

Although most agencies required vendors to adhere to the state's IT security standards, none of the agencies verified compliance with these standards in accordance with contractual provisions

As noted on page 9, five contracts involving four agencies included language requiring vendor adherence to the state's IT security standards. Leading practices suggest agencies should acquire evidence to verify vendor compliance. For example, compliance audits of the vendor would help agencies determine whether vendors are meeting state IT security requirements.

Although many of the agencies included provisions requiring compliance with state IT standards in their contracts, none of the agencies verified that compliance occurred. They cited several issues:

- **In the agencies' opinion, the state's standards are not always clear.** All five agencies reported several state IT security standards are not sufficiently specific to prescribe clear standards for vendors to implement and agencies to monitor. Four agencies said they would like additional guidance for areas like the risk assessment and for access and authentication-type definitions.

- **Agencies said that in some areas, the state standards are too prescriptive and outdated.** Three agencies mentioned the standards, which were written in 2008, though updated from time to time, have not kept up with some changes in technology and evolving policy needs. For example, security personnel at four agencies reported the state's IT security access and authentication requirements are very prescriptive and outdated. Agencies have struggled to interpret and apply them to their vendors.
- **According to some agencies, OCIO feedback and guidance are not consistent.** Agency staff at four agencies said feedback and guidance from OCIO regarding compliance with the standards varies, and not all standards are consistently interpreted over time. Three agencies said this leads to delays in the application development process, complicated relations with vendors and, in some cases, higher project costs.
- **Vendors who can demonstrate compliance with more common, nationally recognized frameworks are unwilling to comply with individual IT security requirement frameworks.** Vendors can be based outside of the United States, or work with many clients in other states. Some of these vendors have reported they cannot comply with and provide assurance of compliance with the unique security requirements for each of their clients.

OCIO staff agreed with some of the agencies' concerns. However, it also noted some of the controls required in the state IT security standards were developed specifically for the state's IT environment and incorporate the contributions of over 50 statewide IT professionals. Additionally, according to OCIO staff, some of the prescriptive standards are mandated by other stakeholders, such as the Legislature and the Technology Services Board, an advisory board to OCIO that provides strategic advice and guidance.

Most of the agencies in our audit suggested allowing other federal or other nationally recognized standards to substitute for compliance with parts of the state's IT security standards, while still keeping some of the stringent and specific OCIO requirements. Agencies said that some of the alternative standards have clearer guidance and more frequent updates, and are comparable to OCIO standards regarding security.

Creating a forum that would include representatives from the OCIO and agencies' IT personnel might help OCIO better understand agencies' IT vendor-related concerns and take them into consideration when updating and improving state IT security standards. It also could help the agencies better understand the constraints that OCIO must consider when working on the standards.

Several agencies could do more to specify responsibilities and roles, and to communicate regularly with vendors about IT security

Leading practices state that agencies should establish clear communication protocols in the contract that articulate the roles and responsibilities of the project managers from both parties, as well as how they will communicate. The roles of agency and vendor IT staff could be outlined in the contract or a separate document, such as a communication plan. Clear and formalized communication protocols are essential to good contract monitoring. They provide clarity, build relationships and are a venue for appropriate ongoing vendor monitoring. They are especially important when there is turnover at the agency or at the vendor.

As **Exhibit 2d** shows, agencies articulated the roles and responsibilities of both parties for three contracts. Specifically, they listed roles and responsibilities of project managers and staff responsible for IT security monitoring. These roles and responsibilities were very detailed and specified either in the contract or other documents, for example, a communications plan or project management plan.

Exhibit 2d – State agencies' IT security monitoring efforts

	Agency letter / contract number						
Requirements	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**
Managers' roles and responsibilities included in the contract	✓	✓	×	✓	×	×	✓
IT *staff* roles and responsibilities included in other documents	✓	✓	×	×	×	×	✓

✓ *means the contract* ***included*** *the requirement.*
× *means the contract* ***did not include*** *the requirement.*

One agency indicated project managers' roles for both parties in the contract. It also created an agency contact list that listed some roles and responsibilities of staff. However, the agency did not include the staff responsible for IT security monitoring in any of these documents. The agency said it did not formalize the roles and responsibilities of staff responsible for IT security monitoring as doing so in the contract would require issuing contract amendments each time a new person fills in the position. However, the agency acknowledged the importance of formalizing staff roles and responsibilities in other ways, such as creating a communications plan.

Two agencies responsible for three contracts did not articulate specific roles and responsibilities either in the contract or another supplemental document. At one agency it was reported when developing the contract, the agency was not clear what the roles and responsibilities would be and the IT security manager left during this process. Staff noted roles and responsibilities are still changing, and they are considering formalizing them through a future amendment to the contract. For another contract, the agency did not include any staff roles and responsibilities as it did not see a need to formalize them because both the vendor and the agency know the main points of contact at each side.

Another agency considers its contract to be low risk based on the maturity of the application, IT security certifications and 24/7 vendor support. Thus, the agency does not plan to formalize staff roles and responsibilities. However, we noted it was not clear exactly which staff at the agency are responsible for monitoring IT security of the application.

Though agencies did not formalize staff roles and responsibilities in some of the contracts, staff at most of the agencies know who is responsible for IT security monitoring as it relates to each of these specific contracts. However, should those employees leave, the agency's monitoring activities and communication with the vendor could be affected, because new employees might not be aware of informally agreed upon responsibilities.

Agencies regularly communicated with contractors. However, more consistent communication with vendors about IT security would improve monitoring efforts

Agencies established formal communication protocols for four of the seven contracts. Following these protocols, they regularly communicated with their vendors. In addition to regular communication via phone, email, mail or video conference, the agencies held regular status meetings with their vendors, required their vendors to submit periodic reports, and conducted routine visits to the vendors' facilities.

Two agencies did not formalize communication protocols with their vendors for three contracts. One agency responsible for two contracts said it does not anticipate much need for the communication with the vendor for one contract, though agency personnel do talk to the vendor. For the second contract, the agency said the communication process is being revised. However, once that process is completed, it can be formalized by amending the contract.

Another agency responded its project manager knows the channels of communication with the vendor and it does not see the need to formalize them.

Though agencies regularly communicate with their contractors, the majority discuss IT security only on an ad hoc basis, for example, once or twice a year. Agencies believe that this is sufficient communication based on the type of application. However, having deliberate IT security conversations with the vendor, including planned meetings and other communications, may allow the agency to gather additional information and increase the likelihood the agency will address any IT security issues in a timely manner with the vendor.

Exhibit 2e summarizes which contracts met clear communication protocols criteria.

Exhibit 2e – State agencies' IT security monitoring efforts

	Agency letter / contract number						
Requirement	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**
Clear communication protocols established	✓	✓	×	✓	×	×	✓

✓ *means the contract* ***included*** *the requirement.*
× *means the contract* ***did not include*** *the requirement.*

DES could help agencies manage IT contracts more effectively by including specific IT guidance in its policies and procedures for contracting

DES is currently developing formal policies with regard to contract monitoring, and plans to deliver a training on leading practices for procurement specialists. However, the new training program was put on hold for further revisions, and DES does not know when it will be available. In addition, the training will focus on general contract monitoring and will not be specific to IT security. While general contract monitoring guidance is helpful, a few of the agencies stated including specific IT guidance in DES contracting policies and procedures as well as in the training would be helpful in improving agency contract management and oversight of IT vendors.

In addition to formal policies and guidance from DES, some agencies also suggested creating a forum where agencies can exchange experiences and leading practices in IT vendor contract monitoring and learn from each other. These agencies suggested the OCIO could host the forum.

What contractual provisions have selected state agencies included in vendor contracts to protect the state in case of a data breach?

Answer in brief

Indemnification clauses, notification clauses and cyber-liability insurance are good tools to protect the state, but there are no agreed-upon standards for these. All seven contracts included indemnification language to protect the state in the event of a data breach, but the language could be improved for some contracts and one contract had especially good language. OCIO has some good indemnification language agencies can use, but agencies have to request it. Additionally, the required timelines for notifying the state of a data breach in most contracts were longer than the state's security policies would suggest. Finally, we noted one contract required cyber-liability insurance, and two other vendors carry the insurance.

Indemnification clauses, notification clauses and cyber-liability insurance are good tools to protect the state, but there are no agreed-upon standards for these

Three ways to limit the liability of the state in the event of a breach are indemnification clause, notification clause and cyber-liability insurance. An indemnification clause clarifies who is contractually responsible to pay for costs in the event the vendor experiences a security breach involving the state's confidential information. Notification clauses define timelines for reporting a security breach. Cyber-liability insurance directly protects the vendor in the event of a security breach by paying some or all the breach related costs. When a vendor carries cyber-liability insurance it also indirectly protects the state, by providing further assurance the vendor may be able to cover costs in the event of a data breach.

While indemnification and notification clauses are important to protecting the state, there is no recommended language for agencies to use when contracting with IT vendors. Similarly, there is no agreed-upon standard for when cyber-insurance should be used. As a result, we considered stakeholders' input to determine which assurances would be most helpful to report on. Thus, we reviewed notification and indemnification clauses to determine if they were clearly written to protect the state by:

- Holding the vendor contractually responsible for costs in the event of security breach
- Requiring vendors to provide the state with timely notification about the security breach
- Identifying roles and responsibilities of vendors' subcontractors in case of a security breach

We also reviewed the contracts to see if agencies were requiring vendors to carry cyber-liability insurance to provide further assurance vendors may be able to cover the contractual obligations in the event of a data breach. **Exhibit 3** summarizes the assurances contained in these agencies' contracts.

Exhibit 3 – Contract assurances in case of a data breach

Five agencies (A – E), with seven contracts (1 – 7) in total

	Agency letter / contract number							
Contract assurance	**A/1**	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**	**Total**
Cyber-liability insurance required	×	×	×	×[1]	×[1]	×	✓	**1/7**
Indemnification and notification clauses included	✓	✓	✓[2]	✓	✓[2]	✓	✓	**7/7**
Mention of subcontractors and their responsibilities	✓	✓	✓	✓	×	✓	✓	**6/7**
Data breach defined	✓	✓	×	×	✓	✓	✓	**5/7**
Data breach notification timeline	5 days[3]	24 hours	2 calendar days	"immediately"	Immediately – not later than 5 business days	Immediately – not later than 5 calendar days	Promptly – not later than 30 calendar days	**7/7**
Party responsible for notifying affected people	Vendor	Vendor	Vendor	Vendor	Vendor	Vendor	Vendor	**7/7**
Party responsible for covering costs	Vendor	Vendor	Not addressed[4]	Vendor	Vendor	Vendor	Vendor	**6/7**
Monetary penalty for data breach	✓	✓	×	×	×	×	×	**2/7**

✓ *means the contract* ***included*** *the requirement.*

× *means the contract* ***did not include*** *the requirement.*

1. Vendors provided the agency cyber-liability insurance though it was not a requirement in their contracts.
2. Contract contains conflicting language; in one case, contract used an order of precedence to resolve the conflict.
3. Contract does not specify business or calendar days.
4. Not addressed in the contract.

All seven contracts included indemnification and notification language to protect the state in the event of a data breach, but the language could be improved for some contracts

It is important to clearly define vendor obligations. For example, the indemnification and notification clauses should clearly define what constitutes a data breach, provide a clear timeline for when a security breach should be reported to the state, and identify who will be responsible for costs associated with a security breach. Well-written indemnification and notification clauses:

- Establish clear roles and responsibilities of the contracted parties
- Help provide assurance the state will be notified quickly, and therefore be involved in all incident management efforts
- Will provide the state with added assurance the vendor will cover the contractual obligations in the event of a data breach

While all seven contracts included indemnification and notification language to protect the state, we noted some contracts could benefit from additional clarity. For example:

- One contract noted the vendor was responsible for costs associated with a data breach, but also included language that the vendor and the state would hold each other harmless.
- A second contract contained conflicting indemnification clauses. Although the same contract did specify which agreement takes precedence in the event of a conflict, a better practice going forward would be to remove the conflicting language from the contract. In addition, the indemnification language in this contract did not specify which party was responsible for costs associated with a data breach.
- Two contracts did not define a data breach, which is important in the event that obligations in the contract are triggered.

On the other hand, one contract had especially good language to protect the state

One contract reviewed also included very clear and detailed indemnification and notification language. For example, the contract:

- Defines a security breach
- Requires quick (24 hours) notification of the state agency about the security breach
- States subcontractors' responsibilities in case of a data breach
- Holds the vendor responsible for all costs associated with a security breach
- Identifies the vendor as responsible for notifying people affected by the breach, as approved by the agency

We have shared this contract with the state's Office of Risk Management at DES so it may be used in future IT contracts at other state agencies.

OCIO has some good language agencies can use, but they have to request it

The OCIO reported it has developed indemnification language agencies can, but are not required to, use when developing contracts. This language is available if requested, and the OCIO recommends agencies have their Assistant Attorneys General review the language if the agency chooses to use it.

The required timelines for notifying the state of a data breach in most contracts were longer than the state's security policies would suggest

When an application is outsourced to a vendor, the state must rely on the vendor to communicate if and when confidential information has been compromised. There are no definitive standards in the state for what is fast enough. State law requires private businesses to notify the owner of the data, in this case the state, immediately following discovery of a data breach (RCW 19.255.010(2)), but essentially leaves it up to the parties to decide what "immediately" means. OCIO requires agencies to notify the state Chief Information Security Officer within 48 hours of a security incident (OCIO policy 143).

For our purposes, we used 48 hours as a reasonable timeline for reporting a data breach because a data breach is a type of serious security incident. In the review of the seven contracts, only two required notification within 48 hours as shown in Exhibit 3 (page 21). Specifically:

- Two contracts required notification within two days, which is consistent with the state policy requirement.
- Three contracts required notification within five days. A fourth contract required notification within a month, which is not consistent with the state policy requirement.
- The final contract required notification "immediately," but did not define a clear timeframe.

Allowing a vendor five days or more to notify the agency of a breach is not consistent with the state's policy of addressing and mitigating these situations quickly. To mitigate the potential effect of a data breach or security incident involving state-owned data, it is essential the state be involved in incident management efforts quickly, which requires early notification. In addition to potential noncompliance, delayed notification of state officials can have severe consequences and significantly increase the state's liabilities.

One contract required cyber-liability insurance, and two other vendors carry the insurance

Each contract for a vendor-hosted application carries different risks to the state. While a robust indemnification clause is one of the most important contractual tools agencies can use to protect the state, agencies need to consider a vendor's capacity to pay in the event of a large data security breach, or a good indemnification clause might not fully protect the state. For example, if an agency is contracting with a small vendor serving many states, and the vendor experiences a data breach affecting large amounts of data from many states, the vendor may be unable to pay the costs it is contractually responsible for, which would leave the state responsible for the costs. For this reason, agencies should consider conducting financial due diligence on prospective vendors, to assess whether the vendor would be able to meet their contractual obligations in the event of a breach. This assessment can then be used to also consider whether to require cyber-liability insurance to further protect the state.

Security incident is an event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.

Data breach is a serious type of security incident that involves the release of personally sensitive, protected and/or confidential data, such as Social Security numbers and personal health records.

To help determine when cyber-liability insurance might be necessary, state agencies can discuss the contract risk with the DES Office of Risk Management and their Assistant Attorneys General. The DES Office of Risk Management has also developed Cyber-Liability Insurance Contracting Considerations guidance for agencies to reference when considering insurance. In addition, the state purchases property insurance, which includes limited cyber-liability insurance. Agencies that participate in the state property insurance thus have some cyber-liability insurance that can be used if a data breach occurs. Agencies can consider this insurance when developing appropriate contract requirements.

We did not attempt to determine whether agencies should have required their vendors to carry cyber-liability insurance. Such determination would require a financial analysis of the vendors and a risk assessment of the application that was beyond the scope of this audit. However, for informational purposes, we did review the contracts to determine whether or not the agencies were requiring such insurance to provide further assurance the vendor will be able to meet their contractual obligations in the event of a data breach. Out of the seven contracts, one contract required the vendor to carry cyber-liability insurance, and two other vendors had cyber-liability insurance although it was not a requirement in their contracts.

State Auditor's Conclusions

When state agencies contract with IT vendors, the agencies can save the resources they would otherwise need to develop applications themselves. However, when agencies outsource IT applications, they must take reasonable steps to ensure their vendors treat the public's data with the appropriate level of care.

That is where the contracts for services become important. The legal contracts between agencies and their vendors should include appropriate provisions to protect the public's information. As this audit shows, most state agencies use contract management practices that fall short of what is needed in the cybersecurity realm. The agencies we reviewed did not conduct the types of formal risk assessments that are needed to identify appropriate security provisions to include in their contracts; nor did they consistently use the provisions that were in the contracts to monitor their vendors' performance.

While state agencies are ultimately responsible for the security of the data they outsource to vendors, they need better support in the form of clear guidance, standards and draft language to use in their contracts. The Office of the Chief Information Officer (OCIO) and the Department of Enterprise Services should develop draft language about several important elements that should be included in every IT contract. These elements could include defining "security breach," setting notification expectations, and specifying how a vendor will compensate the public if something goes wrong.

Finally, the OCIO should clarify the state IT security standards and provide more guidance to the state agencies to help ensure they include compliance requirements with appropriate state IT security standards in their contracts. Additionally, the OCIO should examine alternatives to its current requirement that vendors meet the state's IT security standards. Vendors and agencies view some of the state's security guidelines as either too broad or too prescriptive. One solution would be to accept vendors that can demonstrate compliance with nationally recognized IT security frameworks or federal IT security standards instead.

Recommendations

We recommend the Department of Enterprise Services (DES):

1. Create recommended contract draft language, in cooperation with OCIO, that agencies can use to satisfy basic state IT security requirements when developing new contracts. When completed, share the recommended language with the Office of the Attorney General and agencies' staff responsible for contract monitoring.

This recommendation will help ensure contracts with IT vendors comply with state laws and policies and adequately protect the state (see pages 8-11).

2. Finalize policies and procedures to help agencies monitor IT contracts effectively and efficiently.
3. As an agency responsible for contracting policies, consider creating a forum for agency IT and contracting professionals and OCIO staff to share leading practices, and discuss challenges related to ensuring IT security over vendor-hosted applications.

These recommendations will help ensure agencies monitor their contracts with vendors on an ongoing basis throughout the life of the contract (see pages 12-19).

4. Work with the Office of the Attorney General and OCIO to help develop recommended indemnification and notification language. Among other things, such language should clearly define a security breach, timelines for reporting a security breach, and the responsibility of each party in the event of a security breach. When completed, share the recommended language with the state agency procurement officers.

This recommendation will help ensure the state is protected in case of a data breach (see pages 20-24).

We recommend the Office of the Chief Information Officer (OCIO):

5. Continue to clarify state IT security standards to help agencies determine how to ensure vendor compliance both before and after the application is deployed. That way, agencies can gain assurance that vendors hosting applications are securely processing and storing confidential state data.
6. Determine if additional nationally recognized IT security frameworks or federal IT security standards could substitute for all or part of the state's IT security standards in IT vendor contracts.
7. Clarify expectations for the IT risk assessment that agencies must submit during the security design review process, by providing additional written guidance and tools.

These recommendations will help agencies ensure the security of confidential data in vendor-hosted applications and vendor compliance with the state IT security standards (see pages 8, 10, 15 and 16).

8. Provide uniform guidance on how agencies should interpret the term "immediately" in RCW 19.255.010(2) so agencies can include consistent notification timeline requirements in contracts with their vendors. This recommendation will help ensure the state is protected in case of a data breach (see pages 20-24).

We recommend the audited state agencies:

9. Continue to work to ensure the security of confidential data in vendor-hosted applications (see pages 8-11) by:
    a. Conducting a risk assessment to identify appropriate state and agency IT security requirements for each vendor-hosted application and require vendors to comply with them. If certain security requirements do not apply to a vendor-hosted application, the agency should confirm with the OCIO that those standards may be omitted by submitting a waiver request to the state Chief Information Security Officer (CISO).
    b. Including the requirement for compliance with appropriate state and agency IT security requirements in the solicitation process so all potential vendors are fully aware of the requirement from the beginning of the procurement process and are able to respond accordingly.
    c. If vendors are unable to comply with one or more IT security requirements, agencies should work with the vendor to identify controls that are commensurate with the requirements. Agencies should then submit a waiver request to the state CISO identifying the specific section of OCIO 141.10 that cannot be met, along with any information relating to compensating controls.
    d. In cases where agencies' vendors comply with alternative IT security frameworks, agencies should demonstrate compliance by mapping comparable contractor controls to all appropriate IT security standards and controls, and add supplemental controls to close any gaps between state standards and other IT security frameworks in place.
    e. Requesting a security design review in accordance with criteria outlined in OCIO 141.10 to help ensure vendors secure state data and assets appropriately and comply with state IT security standards before implementing vendor-hosted applications.
10. Improve the monitoring of vendors (see pages 12-19) by following leading practices on contract monitoring. Specifically:
    a. Using results of the conducted risk assessment, develop appropriate contractual monitoring criteria, including details outlining how, and how often, the vendor should demonstrate compliance.
    b. Verify vendor compliance with IT security requirements stated in the contract, in accordance with contractual timelines and using the tools and processes detailed in the contract.
    c. Develop and formalize communication protocols with their vendors that include:
        - Clear roles and responsibilities for agency and vendor staff as they relate to IT security.
        - Clear channels of communication between the agency and the vendor as well as types and frequency of communication regarding IT security in particular.

11. To protect the state in the event of a security breach (see pages 20-24), we recommend state agencies:
    a. Continue working with the DES Office of Risk Management and Assistant Attorneys General when developing contracts to ensure robust indemnification and notification language and to consider when cyber-liability insurance might be appropriate.
    b. Ensure the data breach notification timeline in the current and future contracts aligns with state laws and policies.

Guidance for all Washington state agencies

We consider the audit results so broadly applicable that it is in the state's best interest for every state agency to undertake the actions communicated to the few that participated directly in the audit. We therefore suggest all Washington state agencies consider the *Recommendations to audited agencies* as they develop IT contracts in the future.

Agency Response

JAY INSLEE
Governor

STATE OF WASHINGTON

WASHINGTON TECHNOLOGY SOLUTIONS

1500 Jefferson Street SE • Olympia, Washington 98504-1501

December 10, 2018

The Honorable Pat McCarthy
Washington State Auditor
P.O. Box 40021
Olympia, WA 98504-0021

Dear Auditor McCarthy:

On behalf of the audited agencies and the Department of Enterprise Services (DES), thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report, "Contract Assurances for Vendor-Hosted State Information Technology Applications."

We appreciate the recommendations provided by the SAO and agree there are opportunities to improve and learn from. The SAO's recommendations will help DES and the Office of the Chief Information Officer (OCIO) improve their processes and tools, which will more broadly help state agencies, improve the security of sensitive information entrusted to the state.

In general, we agree the recommendations to the agencies in the audit are good practices for all state agencies. However, we caution that the results the SAO identified through auditing five agencies and seven contracts should not be broadly construed as results for all state agencies. For example, in one specific case only one contract was reviewed for an agency where the vendor was a sole provider of a required service where the vendor did not comply with all requirements. Basing results broadly on such a narrow scope of review may not be a fair representation of whether an agency complies with IT security requirements.

Some of the audited agencies have already made improvements and more are underway. Steps to be taken to address SAO's recommendations follows.

Please thank your team for their important work on this performance audit.

Sincerely,

James Weaver
Director & State Chief Information Officer

cc: David Postman, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Drew Shirk, Executive Director of Legislative Affairs, Office of the Governor
Keith Phillips, Director of Policy, Office of the Governor
Inger Brinck, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
John Cooper, Senior Performance Project Manager, Results Washington, Office of the Governor
Scott Bream, Acting Chief Information Security Officer, Washington Technology Solutions
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor

Official State Cabinet Agency Response to Performance Audit on Contract Assurances for Vendor-Hosted State Information Technology Applications – December 10, 2018

This management response to the State Auditor's Office (SAO) performance audit report received November 16, 2018, is provided by the Office of the Chief Information Officer (OCIO) on behalf of the audited agencies and the Department of Enterprise Services.

SAO Performance Audit Objectives:

The SAO assessed whether:

1. Selected IT contracts have included appropriate provisions to address the state's IT security requirements?
2. Selected state agencies follow leading practices to ensure vendors comply with the IT security requirements in their contracts?

   The SAO also examined:

3. What contractual provisions selected state agencies have included in vendor contracts to protect the state in case of a data breach?

SAO Recommendations 1-4 to the Department of Enterprise Services (DES):

1. Create recommended contract draft language, in cooperation with OCIO that agencies can use to satisfy basic state IT security requirements when developing new contracts. When completed, share the recommended language with the Office of the Attorney General and agencies' staff responsible for contract monitoring.
2. Finalize policies and procedures to help agencies monitor IT contracts effectively and efficiently.
3. As an agency responsible for contracting policies, consider creating a forum for agency IT and contracting professionals and OCIO staff to share leading practices, and discuss challenges related to ensuring IT security over vendor-hosted applications.
4. Work with the Office of the Attorney General and OCIO to help develop recommended indemnification and notification language. Among other things, such language should clearly define a security breach, timelines for reporting a security breach, and the responsibility of each party in the event of a security breach. When completed, share the recommended language with the state agency procurement officers.

STATE RESPONSE: The Department of Enterprise Services (DES) recognizes the value of the Auditor's recommendations as they pertain to DES and fully supports working with the Office of the Chief Information Officer and the Office of the Attorney General to implement the recommendations.

DES offers a basic contract management training and is in the process of developing an advanced contract monitoring training, which will include procedures. An enterprise contract management and monitoring policy will be also be adopted.

DES will also consider creating a forum for agency IT contracting professionals and OCIO staff to share leading practices and to discuss the challenges related to ensuring IT security over vendor-hosted applications.

Action Steps and Time Frame

- Work with the OCIO and the Attorney General's Office (AGO) to draft recommended contract language for agencies to address basic state IT security requirements for new contracts. This will include indemnification and notification language. *By July 1, 2019.*
- Develop an advanced contract management training, to include procedures. *By July 1, 2019.*
- Adopt an enterprise contract management and monitoring policy. *By December 31, 2019.*
- Consider creating a forum for agency IT contracting professionals and OCIO staff to share leading practices and discuss challenges related to ensuring IT security over vendor-hosted applications. *By December 31, 2019.*

SAO Recommendations 5-8 to the Office of the Chief Information Officer (OCIO):

5. Continue to clarify state IT security standards to help agencies determine how to ensure vendor compliance both before and after the application is deployed. That way agencies can gain assurance that vendors hosting applications are securely processing and storing confidential state data.
6. Determine if additional nationally recognized IT security frameworks or federal IT security standards could substitute for all or part of the state's IT security standards in IT vendor contracts.
7. Clarify expectations for the IT risk assessment that agencies must submit during the security design review process, by providing additional written guidance and tools.
8. Provide uniform guidance on how agencies should interpret the term "immediately" in RCW 19.255.010(2) so agencies can include consistent notification timeline requirements in contracts with their vendors.

STATE RESPONSE: The Office of Cyber Security (OCS) will continue to encourage agencies to participate in OCS monthly technical and policy training sessions, and weekly open office hours to address security issues. This includes education for agencies on steps they can take to ensure vendor compliance both before and after new systems are deployed.

Existing OCIO security standards are tailored to address Washington State's specific IT environment and are closely aligned with Federal IT standards. However, OCIO will investigate to determine where Federal standards could be used explicitly to substitute for part of the state's IT security standards in vendor contracts in order to establish "common language" and frame of reference for vendors who have already achieved compliance with Federal standards. The OCIO will also investigate risk assessment tools agencies can use to better understand their vulnerabilities, and work with agencies to develop these tools.

The OCS will work with DES contracts and state agencies to develop guidance and consensus on how the term "immediately" should be interpreted in order to provide consistent notification timeline requirements in contracts with vendors.

Action Steps and Time Frame

- Continue to educate and clarify for agencies steps they can take to ensure vendor compliance. *Ongoing.*
- Investigate where Federal standards could be used to explicitly substitute for part of the state's IT security standards in vendor contracts to establish "common language" and frame of reference for vendors who are compliant with Federal standards. *By December 31, 2019.*
- Investigate risk assessment tools agencies can use to better understand their vulnerabilities and work with agencies to develop these tools. *By September 30, 2019.*
- Work with DES contracts and state agencies to develop guidance on how the term "immediately" should be interpreted in order to provide consistent notification timeline requirements in contracts with vendors. *By July 1, 2019.*

SAO Recommendations 9-11 to state agencies:

9. Continue to work to ensure the security of confidential data in vendor hosted applications.
    a. Conducting a risk assessment to identify appropriate state and agency IT security requirements for each vendor-hosted application and require vendors to comply with them. If certain security requirements do not apply to a vendor-hosted application, the agency should confirm with the OCIO that those standards may be omitted by submitting a waiver request to the state Chief Information Security Officer (CISO).
    b. Including the requirement for compliance with appropriate state and agency IT security requirements in the solicitation process so all potential vendors are fully aware of the requirement from the beginning of the procurement process and are able to respond accordingly.
    c. If vendors are unable to comply with one or more IT security requirements, agencies should work with the vendor to identify controls that are commensurate with the requirements. Agencies should then submit a waiver request to the state CISO identifying the specific section of OCIO 141.10 that cannot be met, along with any information relating to compensating controls.
    d. In cases where agencies' vendors comply with alternative IT security frameworks, agencies should demonstrate compliance by mapping comparable contractor controls to all appropriate IT security standards and controls, and add supplemental controls to close any gaps between state standards and other IT security frameworks in place.
    e. Requesting a security design review in accordance with criteria outlined in OCIO 141.10 to help ensure vendors secure state data and assets appropriately and comply with state IT security standards before implementing vendor-hosted applications.
10. Improve the monitoring of vendors by following leading practices on contract monitoring. Specifically:
    a. Using results of the conducted risk assessment, develop appropriate contractual monitoring criteria, including details outlining how, and how often, the vendor should demonstrate compliance.
    b. Verify vendor compliance with IT security requirements stated in the contract, in accordance with contractual timelines and using the tools and processes detailed in the contract.
    c. Develop and formalize communication protocols with their vendors that include:
        - Clear roles and responsibilities for agency and vendor staff as they relate to IT security.

- Clear channels of communication between the agency and the vendor as well as types and frequency of communication regarding IT security in particular.

11. To protect the state in the event of a security breach, we recommend state agencies:
    a. Continue working with the DES Office of Risk Management and Assistant Attorneys General when developing contracts to ensure robust indemnification and notification language and to consider when cyber liability insurance might be appropriate.
    b. Ensure the data breach notification timeline in the current and future contracts aligns with state laws and policies.

STATE RESPONSE: We appreciate and agree with the recommendations provided by the SAO. While we are unable to modify the conditions of our current contracts to address all of the recommendations, we plan to address these in contract amendments and operational processes as appropriate. Going forward we plan to take the following actions to improve future contracts.

Action Steps and Time Frame
For future contracts, the audited agencies plan to take the following actions by the designated date:

- Develop a process for conducting risk assessments, to include state and agency IT security requirements (agencies 1-5). *By March 31, 2020.*
- Include in RFPs for vendor-hosted applications the requirement for compliance with applicable agency, state, and federal IT security requirements (agencies 2, 3, 4 and 5). *By July 1, 2019*
- Develop a process to work with vendors unable to comply with IT security requirements to submit a waiver request to the state's Chief Information Security Officer (agencies 1-5). *By March 31, 2020.*
- Develop a process or continue to work with vendors who are complying with alternative IT security frameworks to demonstrate full compliance with the required IT security standards (agencies 1-5). *By March 31, 2020.*
- Continue to or request a security design review in accordance with criteria outlined in the state's IT standards OCIO 141.10 (agency 3, 4, and 5). *By March 30, 2020.*
- Use the results of risk assessments conducted to develop appropriate contractual monitoring criteria (agencies 1-5). *By May 1, 2020.*
- Verify vendor compliance with IT security requirements using contractual timelines, tools and processes (agencies 1, 3 and 5). *By July 1, 2019.*
- Develop communication plans for contracts that identify roles and responsibilities of agency and vendor representatives, as well as how and when they communicate (agencies 3 and 5). *By May 1, 2020.*
- Continue to or develop a process to work with the DES Office of Risk Management and the AGO when developing contracts and consider cyber liability insurance where appropriate (agencies 1-5). *By March 31, 2020.*
- Work with DES and OCIO to develop guidance on how the term "immediately" should be interpreted and ensure data breach notification timelines are included in all future contracts that align with state laws and policies (agencies 1-5). *By July 1, 2019.*
- Work with DES and OCIO to develop guidance to follow when vendors don't comply with IT security requirements, especially in circumstances where a vendor is the sole provider of a required service or where purchase of the product requires use of a click-through website that does not allow for review and acceptance of IT security requirements (agency 3 and 5). *By March 31, 2020.*

Appendix A: Initiative 900 and Auditing Standards

Initiative 900 requirements

Initiative 900, approved by Washington voters in 2005 and enacted into state law in 2006, authorized the State Auditor's Office to conduct independent, comprehensive performance audits of state and local governments.

Specifically, the law directs the Auditor's Office to "review and analyze the economy, efficiency, and effectiveness of the policies, management, fiscal affairs, and operations of state and local governments, agencies, programs, and accounts." Performance audits are to be conducted according to U.S. Government Accountability Office government auditing standards.

In addition, the law identifies nine elements that are to be considered within the scope of each performance audit. The State Auditor's Office evaluates the relevance of all nine elements to each audit. The table below indicates which elements are addressed in the audit. Specific issues are discussed in the Results and Recommendations section of this report.

I-900 element		Addressed in the audit
1.	Identify cost savings	**No.** The audit objectives did not include identifying cost savings.
2.	Identify services that can be reduced or eliminated	**No.** The audit focused on contract assurances related to the security of state data maintained in vendor databases, and reports on the assurances that agencies include in their contracts in case of a security data breach.
3.	Identify programs or services that can be transferred to the private sector	**No.** The audit reviewed services that have already been transferred to private IT vendors.
4.	Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**Yes.** State OCIO IT security standards require agencies to hold their vendors accountable for complying with those IT security standards. The audit concludes that not all reviewed contracts included such a compliance requirement. The agencies must follow the requirement by including appropriate contractual language and monitoring to ensure compliance.
5.	Assess feasibility of pooling information technology systems within the department	**No.** The audit focused on agencies' IT vendor contract controls, not pooling their information technology systems.
6.	Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**Yes.** This audit concludes the agencies should follow leading practices to strengthen their oversight of state IT vendors and their contracts. It also concludes the state oversight agencies need to clarify the guidance for state agencies related to IT security standards and contract monitoring.
7.	Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.** However, the audit recommends the OCIO provide uniform guidance on how agencies should interpret the term "immediately" in RCW 19.255.010(2), so agencies can include consistent notification timeline requirements in contracts with their vendors.
8.	Analyze departmental performance data, performance measures and self-assessment systems	**No.** This audit did not analyze performance data, measures or systems. The audit focused on examining contract assurances to protect state IT applications' managed by third-party vendors.
9.	Identify relevant best practices	**Yes.** As part of this audit, we identified leading practices related to IT vendor security and oversight of contractors. See Appendix C for detailed leading practices.

Compliance with generally accepted government auditing standards

We conducted this performance audit under the authority of state law (RCW 43.09.470), approved as Initiative 900 by Washington voters in 2005, and in accordance with generally accepted government auditing standards as published in Government Auditing Standards (December 2011 revision) issued by the U.S. Government Accountability Office. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix B: Scope, Objectives and Methodology

Scope

This audit reviewed seven contracts at five state agencies for their vendor-hosted applications that are critical to agencies' missions and contain confidential data.

Objectives

The purpose of the audit is to determine whether agencies are obtaining assurance their contracted IT vendors hosting mission-critical applications with confidential information are safeguarding those systems and the state's data. The audit answers the following questions:

1. Have selected IT contracts included appropriate provisions to address the state's IT security requirements?
2. Do selected state agencies follow leading practices to ensure vendors comply with the IT security requirements in their contracts?

Even with good IT security in place, incidents and breaches can still happen. To assess whether the state is protected in the event of a security breach the audit also examined:

3. What contractual provisions have selected state agencies included in vendor contracts to protect the state in case of a data breach?

Methodology

To answer the audit's three objectives, auditors needed to identify relevant contracts to review, establish criteria to assess the contracts, and consider the actions agencies took to monitor the contracts in consideration of the risks that these vendor-hosted IT applications pose to state IT security.

Agencies and contract selection

Washington does not maintain a master list of all vendor-hosted IT applications we could use to identify contracts to review. Instead, auditors used the results of the Statewide Information Technology Risk Assessment our Office conducted in 2015 to compose a shortlist of selected agencies and the vendor-hosted IT applications the agencies use. We shared the list with state subject matter specialists – the state's Chief Information Security Officer, the state's Chief Information Officer, and the Cyber Loss Prevention Specialist at DES – to gather their input and suggestions.

We selected five agencies with contracts for seven applications that are vendor-hosted, critical to the mission of the agency, and contain confidential state information. When selecting contracts for review, we did not consider other factors, such as risk or monetary value of the contract.

During the audit, we reviewed a variety of contracts for vendor-hosted applications, varying in terms of cost and size. However, because we did not complete an exhaustive search to identify all mission-critical, vendor-hosted, state applications with confidential state information, and used a random sample to choose agency contracts for this audit, it may not be possible to generalize the results of our review across all agencies and IT vendor contracts.

We used the following approaches to address the audit objectives.

Determined agencies' compliance with requirements in OCIO 141.10

OCIO 141.10 requires agencies to include appropriate language in vendor contracts to require the vendor to comply with both the state IT security standards and the agency's own IT security policies. To assess agencies' compliance with these requirements, we reviewed contracts from the selected agencies. In cases where vendor OCIO compliance requirements were not explicit or not stated at all, we reviewed contracts to identify the IT security requirements these contracts included.

Subject matter experts from our Office's IT security team reviewed these contracts to help determine whether they included state IT security standards and compliance requirements. If the contracts did not require vendor compliance with the state and/or agency IT security requirements, we interviewed agency personnel to determine the reasons.

Identified leading practices for IT vendor contract monitoring

We were unable to assess agency compliance with state contract monitoring requirements because DES had not developed them at the time of the audit. Therefore, to identify leading practices for contract monitoring, we used:

- The *Global Technology Audit Guide (GTAG): Information Technology Outsourcing*, a widely recognized guide developed by an International Professional Association of Internal Auditors
- The *Project Management Body of Knowledge (PMBOK) Guide*, a set of widely accepted global standards that provide guidelines and rules for project and program management
- General contract management training materials provided by DES

Reviewed agencies' monitoring practices and processes to identify gaps

To understand agencies' monitoring efforts, we:

- Reviewed contracts to identify monitoring requirements
- Interviewed staff responsible for general contract monitoring and IT security contract monitoring to understand agency monitoring practices
- Reviewed supporting documentation

We then compared what we found to the identified leading contract monitoring practices. Where we found gaps, we looked for potential causes based on interviews and documentation.

Identified contract assurances in the event of a security incident or breach

The state has not issued standards describing what assurances state agencies should include in their contracts to protect the state in case of a data breach, nor is there consensus about when state agencies should require cyber-liability insurance. Therefore, we reviewed contract documents to identify the assurances, such as a cyber-liability insurance requirement and/or specific indemnification and notification language, included in each contract for reporting purposes only. We sought advice of our Office's Director of Legal Affairs when appropriate during this review.

Appendix C: Monitoring and Evaluating Contracts for IT Security – Leading Practices

Vendors hosting systems critical to state agency missions with confidential data must be adequately monitored to gain reasonable assurance that state data is secure and systems will be available to ensure continuity of government operations. Agencies should monitor and evaluate contracts with vendors throughout the life of the contract to ensure compliance with terms and conditions in the contract. We identified leading practices agencies can use to monitor contracts and evaluate vendor-hosted services for IT security.

1. Conduct an IT risk assessment during contract planning and throughout the life of the contract

According to OCIO 141.10, agencies must implement a formal IT risk assessment when introducing new systems, or when changing an existing system in a way that will affect risk. IT risk assessments should also be conducted once every three years for systems processing highly confidential information. Formal IT risk assessments should identify:

- Assets related to the IT security program
- Potential threats to assets within the scope of the program
- Vulnerabilities that might be exploited by threats
- Impacts that losses of confidentiality, integrity and availability may have on program assets
- Likelihood that security failures may occur based on prevailing threats and vulnerabilities

2a. Identify key monitoring requirements

Based on the risk assessment, agencies should establish monitoring requirements or IT security controls to include in the contract to mitigate identified risks. Agencies should also consider which requirements of the state standards in OCIO 141.10 are applicable based on the risks identified. Monitoring requirements should detail the types and frequencies of monitoring events, and can include:

- Third-party audits of security controls
- Penetration testing
- Security scans
- OCIO compliance audits
- Federal certification or security requirements

2b. Include key monitoring requirements in the contract

Monitoring events (HIPAA audit, SOC 2 type 2, IT security audit, etc.) and certifications (FEDRAMP) should be included in the contract, with specified frequency and a requirement to share results with the state. Monitoring requirements and events should also be articulated with more depth in an agency monitoring plan.

Agencies should include a requirement to comply with all relevant state standards from OCIO 141.10 in the contract or maintain a crosswalk mapping comparable vendor controls to relevant OCIO 141.10 controls. Vendors should have a clear understanding of the standards they must comply with, and why.

3. Identify roles and responsibilities, and communication protocols

The roles and responsibilities of contractors and agency contract managers should be well articulated in the contract. The frequency and type of communication should also be clearly specified.

The roles of any additional agency and vendor staff could be outlined in additional documentation, such as a communication plan, which should be shared with the vendor. The plan could specify individuals responsible for reviewing vendor IT security audits and monitor vendor remediation, and identify who will review IT security certifications to ensure they are current.

4. Monitor key contract requirements/assess vendor performance to ensure the security of state data and continuity of state operations

Engage in frequent communication with the vendor and monitor the IT security criteria in accordance with language in the contract. The contract should be monitored by people with clearly identified roles and responsibilities, using criteria that allow the state agency to assess vendor performance, including IT security.

Appendix D: Summary Table of Audit Results

This appendix provides a complete overview of all audit findings and objectives for each contract.

	Agency letter / contract number						
	A/1	**B/2**	**C/3**	**D/4**	**E/5**	**E/6**	**E/7**
Objective 1							
State IT security compliance requirement included	✓[1]	✓	×	✓	✓	×	✓
Agency IT security compliance requirement included	✓	×	×	×	×	×	×
Objective 2							
Risk assessment to identify appropriate IT security monitoring requirements conducted	×	×	×	×	×	×	×
Monitoring requirements included in the contract	✓	✓	×	✓	✓	✓	✓
How to demonstrate compliance specified	Partially	✓	×	✓	×	×	✓
Vendor IT security performance assessed by agency according to monitoring requirements in the contract	✓	✓	×	Ad hoc	×	×	Partially
***Managers'* roles and responsibilities** included in the contract	✓	✓	×	✓	×	×	✓
IT *staff* roles and responsibilities included in other documents	✓	✓	×	×	×	×	✓
Clear communication protocols established	✓	✓	×	✓	×	×	✓
Objective 3							
Cyber-liability insurance required	×	×	×	×[2]	×[2]	×	✓
Indemnification and notification clauses included	✓	✓	✓[3]	✓	✓[3]	✓	✓

*✓ means the contract **included** the requirement.*
*× means the contract **did not include** the requirement.*

1. General statement requiring compliance with all state laws and regulations. 2. Vendors provided the agency cyber-liability insurance though it was not a requirement in their contracts. 3. Contract contains conflicting language; in one case, contract used an order of precedence to resolve the conflict.