Office of the Washington State Auditor
Pat McCarthy

Performance Audit

Contract Assurances for Vendor-Hosted State Information Technology Applications

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 a security design review 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.

Report number 1022707, published 12/13/2018

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

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. OCIO has some good indemnification language agencies can use, but agencies have to request 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. 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 public 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 public 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 (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. 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 the DES to improve the guidance it provides to state agencies that contract for IT services. We also made recommendations to the 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.