Cabinet and Governor Appointed Agencies' Performance Audit Action Item(s) & Status

Contract Assurances for Vendor-Hosted State Information Technology Applications

(See also cabinet agency response for full context to Washington State Auditor's Office (SAO) report, December, 2018)

Five state agencies were included in this performance audit with information also provided by Department of Enterprise Services (DES) and Washington Technology Solutions (WaTech).

SAO Recommendations summary (Rec):

To 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.

To the Office of the Chief Information Officer at WaTech:

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.

To the five audited state agencies:

9. Continue to work to ensure the security of confidential data in vendor hosted applications.
10. Improve the monitoring of vendors by following leading practices on contract monitoring.
11. Continue to work with DES and the Attorneys General to ensure robust indemnification and notification language, and to consider cyber liability insurance. Also ensure that data breach notification timeline in current and future contracts aligns with state laws and policies.

The table below shows the current status of action items the agency initiated to address issues identified in the performance audit report. Please see the *cabinet agency response* for additional context and any additional steps already taken.

For an explanation of the columns below, see the legend.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
Rec. 1-4	Initial complete, potential update in progress	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	DES	7/1/19		N/A	No	Initial language developed in consultation with the AGO is included in the manual for the advanced contract management training program described below. An internal working team within the Contracts and Procurement Division is working to further develop and update such recommended contract language, and will coordinate with the OCIO and AGO in doing so.
Rec. 1-4	Complete	Develop an advanced contract management training, to include procedures	DES	7/1/19		N/A	No	DES Contracts and Procurement Division completed and launched a series of advanced contract management trainings in January 2019. As of July 31, over 5,000 state employees have completed this additional training.
Rec. 1-4	In Progress	Adopt an enterprise contract management and monitoring policy	DES	12/31/19		N/A	No	DES Contracts and Procurement Division's Policy Team is on-track to completing these policies by 12/31/19. Draft policies will be shared publicly at a Workshop on 10/23/19.
Rec. 1-4	In Progress	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	DES	12/31/19		N/A	No	DES Contracts and Procurement Division is considering options for a forum to bring together IT and contracting professionals, and will have a plan for such forum in place prior to 12/31/19.
Rec. 5-8	Ongoing	Continue to educate and clarify for agencies steps	WaTech	N/A	Yes	No	No	**July 2019**: OCS, through its security design review process, works actively with

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
		they can take to ensure vendor compliance						agencies to ensure vendors are compliant with OCIO security standards for all new projects prior to deployment. OCS will continue to work with agencies to further educate them on this requirement.
Rec. 5-8	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	WaTech	~~12/2019~~ On-going	Yes	No	No	**July 2019:** OCS continues to investigate where Federal standards, or equivalent, could be incorporated into the state's IT security standards. OCS is also pursuing the use of the National Cyber Security Framework, which incorporates these federal standards.
Rec. 5-8	Ongoing	Investigate risk assessment tools agencies can use to better understand their vulnerabilities and work with agencies to develop these tools	WaTech	~~9/2019~~ 6/2020	Yes	No	No	**July 2019**: Facilitated by OCS, agencies will be participating in the national CyberSecurity Review Survey in October 2019. The results of this survey will be used to help identify relevant risk assessment tools that can be used to help agencies identify vulnerabilities and additional needed controls.
Rec. 5-8	Ongoing	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	WaTech	~~7/1/ 19~~ 12/2019	Yes	No	No	**July 2019:** OCS has begun discussions with DES contracts to uniformly define what the term "immediately" means. This will result in consistent instruction to vendors as to when security breaches and incidents should be reported to the agency.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
Rec. 9-11	1-In Progress 2-In Progress 3-In Progress 4-In Progress 5-In Progress	Develop a process for conducting risk assessments, to include state and agency IT security requirements	Agencies referred to as "1-5"	3/2020	Yes	No	No	**July 2019:** The state CISO is in the process of chartering an agency CISO council, which will provide the means for agencies to corporately address risk and the means by which it can be measured and evaluated.
Rec. 9-11	2-In Progress 3-In Progress 4-In Progress 5-In Progress	Include in RFPs for vendor-hosted applications the requirement for compliance with applicable agency, state, and federal IT security requirements	Agencies referred to as 2-5	7/2019	Yes	No	No	**July 2019:** The state's IT security standards, from their inception, have included the requirement that contractors comply with these standards. OCS will continue to stress this requirement.
Rec. 9-11	1-In Progress 2-In Progress 3-In Progress 4-In Progress 5-In Progress	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 referred to as 1-5	3/2020	Yes	No	No	**July 2019:** OCS has consistently maintained a process whereby waivers to IT security requirements can be submitted to the state CISO for disposition.
Rec. 9-11	1-In Progress 2-In Progress 3-In Progress 4-In Progress 5-In Progress	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 referred to as 1-5	3/2020	Yes	No	No	**July 2019:** OCS makes available to agencies resources to help assist with the identification of compensating controls when specific compliance requirements cannot be met.
Rec. 9-11	3-In Progress 4-In Progress 5-In Progress	Continue to or request a security design review in accordance with criteria outlined in the state's IT standards OCIO 141.10	Agencies referred to as 3-5	3/2020	Yes	No	No	**July 2019:** OCS has made agencies aware, through language in the states' IT security standards and ongoing workshops, that a security design review is required.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
Rec. 9-11	1-In Progress 2-In Progress 3-In Progress 4-In Progress 5-In Progress	Use the results of risk assessments conducted to develop appropriate contractual monitoring criteria	Agencies referred to as 1-5	5/2020	Yes	No	No	**July 2019**: This is an agency requirement, as OCS does not have the means to monitor ongoing contractor compliance.
Rec. 9-11	1-In Progress 3-In Progress 5-In Progress	Verify vendor compliance with IT security requirements using contractual timelines, tools and processes	Agencies referred to as 1,3,5	7/2019	Yes	No	No	**July 2019:** Individual agencies are responsible for verifying ongoing compliance with stated contractual IT security requirements.
Rec. 9-11	3-In Progress 5-In Progress	Develop communication plans for contracts that identify roles and responsibilities of agency and vendor representatives, as well as how and when they communicate	Agencies referred to as 3,5	5/2020	Yes	No	No	**July 2019:** This is the responsibility of individual agencies depending on the way roles and responsibilities are defined in their contracts.
Rec. 9-11	1-In Progress 2-In Progress 3-In Progress 4-In Progress 5-In Progress	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 referred to as 1-5	3/2020	Yes	No	No	**July 2019:** OCS is providing a workshop to agencies in July 2019, whereby agencies will be provided with guidance from the DES state risk manager. Topics will include cyber liability insurance provided to agencies under the state's policy and how they should incorporate appropriate levels of insurance to be provided by the vendor in their contracts to address loss caused by the vendor.
Rec. 9-11	1-In Progress 2-In Progress 3-In Progress 4-In Progress 5-In Progress	Work with DES and OCIO to develop guidance on how the term "immediately" should be interpreted and ensure	Agencies referred to as 1-5	7/2019	Yes	No	No	**July 2019:** OCS has begun discussions with DES contracts to uniformly define what the term "immediately" means. This will provide consistent instruction to vendors

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
		data breach notification timelines are included in all future contracts that align with state laws and policies						as to when security breaches and incidents should be reported to the agency.
Rec. 9-11	3-In Progress 5-In Progress	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	Agencies referred to as 3,5	3/2020	Yes	No	No	**July 2019**: In cases of non-compliance with state IT security standards, OCS provides resources to agencies to assist them in determining whether compensating controls can be applied in lieu of compliance with the standards, or if a vendor should not be considered based on the absence of controls which would appropriately mitigate risk.