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	In progress, delayed due to COVID-19 response	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	**August 2020:** An internal working team within the Contracts and Procurement Division has met with SAO, ETS, customer agencies and has completed a draft Backgrounder which includes recommended contract language. Partner agencies need additional time to review and comment on the Backgrounder because of the pandemic and DES will continue to coordinate and collaborate with them until the Backgrounder is finalized or an agreement is made to post the draft tool.
Rec. 1-4	Complete	Develop an advanced contract management training, to include procedures	DES	7/1/19		N/A	No	**August 2020:** 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~~ 12/31/20		N/A	No	**August 2020:** DES Contracts and Procurement Division's Policy Team is finalizing the Contract Management policy. The policy draft was impacted by new legislation, delaying the anticipated timeline (HB1521). DES is updating the policy and may need another round of feedback which will push the policy launch to the end of 2020. Note that the material addressed in this policy is largely contained in the training completed in 2019.
Rec. 1-4	In Progress and Deferred	Consider creating a forum for agency IT contracting	DES	12/31/19		N/A	No	**August 2020:** DES had an IT forum in September 2019 and was going to have

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
		professionals and OCIO staff to share leading practices and discuss challenges related to ensuring IT security over vendor-hosted applications						another forum in April 2020, but cancelled the event due to the pandemic. DES is looking at other options, including virtual meetings, to share this information.
Rec. 5-8	Ongoing	Continue to educate and clarify for agencies steps they can take to ensure vendor compliance	WaTech	Ongoing	Yes	No	No	**July 2019**: OCS, through its security design review process, works actively with 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. **August 2020:** This is a core function of the OCS Security Design Review process and OCS will continue to educate agencies on steps they can take to ensure vendor compliance. The State CISO actively educates and advises agencies on the various federal compliance requirements, in addition to the Secure Design Review process, that are required for vendor compliance.
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	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. **August 2020**: OCS currently recognizes certain federally obtained vendor security certifications, such as the Federal Risk and

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
		are compliant with Federal standards						Authorization Management Program (FedRAMP), as substitutes for many of the state's security requirements. OCS is also in the process of revising and replacing the current state IT security standard 141.10 with a national standard that is more aligned with federal standards to fulfill this objective
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~~ On-going	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. **August 2020**: As part of the State CISOs FY 2021 – 2023 State Cybersecurity Operational plan, an initiative identified in that plan is to develop a statewide risk assessment program that provides the necessary procedures and the tools for the agencies to truly understand their vulnerabilities and the priorities in the context of the agency business. CISOs from agencies are also engaged in this effort.
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	WaTech	~~7/1/ 19~~ ~~12/2019~~ 12/2020	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
		requirements in contracts with vendors						**August 2020:** Work was suspended on this pending passage of Substitute House Bill 1071, which updated the state's breach notification laws. The updated law retains the language that vendors must "immediately" notify in the event of a breach. As this is a legal term codified in statute, OCS will work with the Office of the Attorney General, the State Privacy Officer and DES to determine whether a uniform time period (e.g. "24 hours") can be used in all vendor contracts as a means of interpreting "immediately."
Rec. 9-11 (#1)		Develop a process for conducting risk assessments, to include state and agency IT security requirements					**OCIO 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. **OCIO August 2020:** Please see response to related recommendation 5-8 above.	
	In Progress		Agency 1	3/2020	No	Yes	No	The agency security department has in place a procedure to evaluate risk in the context of OCIO 141.10 compliance. Additional work is being done to align the agencies security framework to the NIST Cyber Security Framework model. Risk assessments will include applicable federal security controls as well as the OCIO 141.10 standard. At this time, the security staff position that performs the risk assessments is vacant pending hiring exemption approval.
	Complete		Agency 2	3/2020	Yes	No	No	Built Risk Assessment methodology and templates, conducting recurring Risk Assessments for Agency Services.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
	Complete		Agency 3	3/2020	Yes	No	No	Our process exists and encapsulates the required items listed in OCIO 141.10. Part of the process includes creating and utilizing an IT risk assessment tool which is continually updated to reflect current threats and vulnerabilities.
	Complete		Agency 4	3/2020	Yes	No	No	
	In Progress		Agency 5	04/2021	Yes	No	No	Risk assessment process is still being refined due to conflicting priorities.
Rec. 9-11 (#2)		Include in RFPs for vendor-hosted applications the requirement for compliance with applicable agency, state, and federal IT security requirements					**OCIO 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. **OCIO August 2020:** Complete. This requirement in the state's IT security standards will remain. In addition, OCS advises and educates agencies to include in RFP the applicable federal compliance requirements for the specific vendor-hosted applications.	
	Complete		Agency 2	7/2019	Yes	No	No	Developed standard verbiage to include in RFPs and contracts.
	Complete		Agency 3	7/2019	Yes	No	No	The agency's process for developing, publishing and reviewing RFPs includes current security standards. All competitive solicitations require compliance with applicable agency, state and federal security standards. The RFPs either reference or include links to the OCIO policy site, as well.
	Complete		Agency 4	7/2019	Yes	No	No	
	Complete		Agency 5	7/2019	Yes	No	No	The agency includes a data security element in our IT Procurements.
Rec. 9-11 (#3)		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					**OCIO July 2019:** OCS has consistently maintained a process whereby waivers to IT security requirements can be submitted to the state CISO for disposition.	

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
							August 2020: Complete. OCIO has established Policy 103 which prescribes the process required to submit waivers to all standards and policies, including 141.10.	
	In Progress		Agency 1	3/2020	No	Yes	No	The agency has been and will continue to work with OCS and the OCIO to identify risks and compliance gaps associated with vendor hosted solutions. This includes the completion and submission of Waivers of Non-Compliance for OCIO approval. At this time, the security staff position that performs the risk assessments is vacant pending hiring exemption approval.
	Complete		Agency 2	3/2020	Yes	No	No	
	Deferred		Agency 3	3/2020	Yes	No	No	The agency's IT security office will determine if vendors can meet requirements. If they cannot, the contracts office will not issue the contract. Contractor compliance responses are part of the evaluation and selection process. It's noted that there is a gap in identifying the deviation during the security design review process and submission of the deviation. DOH is looking for OCS to lead this change.
	Complete		Agency 4	3/2020	Yes	No	No	
	Complete		Agency 5	3/2020	Yes	No	No	The agency will work with OCS when necessary for waivers.
Rec. 9-11 (#4)		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					**OCIO July 2019:** OCS makes available to agencies resources to help assist with the identification of compensating controls when specific compliance requirements cannot be met. **August 2020:** Complete. OCS, as part of its Security Design Review function has always provided the means to work	

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
							with vendors who are complying with alternative frameworks, to map those requirements to meet require IT security standards.	
	In Progress		Agency 1	3/2020	No	Yes	No	The agency security group is developing security control crosswalks between the OCIO 141.10 Standard and the federal regulatory controls to which the agency must comply. This crosswalk will allow the security group to effectively and consistently correlate vendor compliance to OCIO 141.10, even when that vendor is using a security framework other than the OCIO 141.10 standard. This work is the result of the agency security group adopting the NIST Cyber Security Framework for its security program. At this time, the security staff position that performs the risk assessments is vacant pending hiring exemption approval.
	Complete		Agency 2	3/2020	Yes	No	No	Leverage a NIST CSF framework crosswalk to facilitate differences in framework taxonomy discussions.
	Complete		Agency 3	3/2020	Yes	No	No	The majority of IT vendors provide via their responses to the RFP that they can comply or will comply with not only OCIO security policies and standards but also with the policies of The agency's IT Security.
	Complete		Agency 4	3/2020	Yes	No	No	
	Complete		Agency 5	3/2020	Yes	No	No	All of our current vendors meet or exceed the current state standard**.**
Rec. 9-11 (#5)		Continue to or request a security design review in accordance with criteria outlined in the state's IT standards OCIO 141.10					**OCIO 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
							August 2020: Complete. The state's IT security standards contain the requirement that agencies submit new services or applications to OCS for a security design review. Though this is an agency responsibility, OCS and OCIO continue to stress this requirement to agencies.	
	Complete		Agency 3	3/2020	Yes	No	No	The agency's operational processes and project management standards were reviewed and updated to ensure security design reviews are conducted when required by policy.
	Complete		Agency 5	3/2020	Yes	No	No	The agency performs design reviews as required by OCIO 141.10
Rec. 9-11 (#6)		Use the results of risk assessments conducted to develop appropriate contractual monitoring criteria (Contracts) (Page 14)					**OCIO July 2019**: This is an agency requirement, as OCS does not have the means to monitor ongoing contractor compliance. **August 2020:** Ongoing. This is an agency responsibility and best practice; however, OCS will continue to work with DES to develop contract language and guidance that provides a process whereby agencies monitor ongoing vendor compliance to contractually mandated security requirements. This should include the requirement that vendors adopt additional controls as needed to address risk throughout the duration of the contract. Procedures to analyze the third-party security controls and requiring the essential monitoring based on that analysis is also part of the statewide risk assessment program implementation that is part of the State CISOs FY 2021-2023 State cybersecurity operational plan.	
	In Progress		Agency 1	5/2020	No	Yes	No	The agency security team works with the agency contracting team on an on-going basis to ensure that appropriate language for OCIO 141.10 compliance is present in all agency contracts with vendors. The agency security and contracting staff will

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
								continue to collaboratively work on contract templates. At this time, the security staff position that performs the risk assessments is vacant pending hiring exemption approval.
	Complete		Agency 2	5/2020	Yes	No	No	Use Risk Assessments to build Plans of Action and Milestones (POAM) documents to track remediation efforts.
	Complete		Agency 3	5/2020	Yes	No	No	The department utilizes multiple sources to develop appropriate contractual monitoring criteria for each contract. Program and IT Security will determine if there are any risks and/or concerns that need to be considered prior to executing the contract. These risks are used to determine if additional monitoring is necessary for that vendor. The additional monitoring criteria is then communicated to contracts to be included in the final contractual document.
	Complete		Agency 4	5/2020	Yes	No	No	
	In Progress		Agency 5	04/2020	Yes	No	No	Risk assessment process is still being refined due to conflicting priorities.
Rec. 9-11 (#7)		Verify vendor compliance with IT security requirements using contractual timelines, tools and processes					**OCIO July 2019:** Individual agencies are responsible for verifying ongoing compliance with stated contractual IT security requirements. **August 2020:** Ongoing. Please see response to recommendation directly above. Procedures to analyze the third-party security controls and requiring the third-parties to submit their audit reports (eg. SOC2) is also part of the statewide risk assessment program implementation that is part of the State CISOs FY 2021-2023 State cybersecurity operational plan.	

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
	In Progress		Agency 1	7/2019	No	Yes	No	As part of the agency security programs alignment to NIST Cyber Security Framework, gaps including this one will be tracked to completion on the security program roadmap. At this time, the security staff position that performs the risk assessments is vacant pending hiring exemption approval.
	Complete		Agency 3	7/2019	Yes	No	No	Vendors agree that technology products and services delivered as part of IT contracts will comply with the Department's information technology standards, as defined in the Technical and Security Requirements of the RFP. The agency's Security reviews this section of the proposal and work with vendors who may have concerns about the requirement.
	Complete		Agency 5	7/2019	Yes	No	No	Contract managers are monitoring and/or alerting IT and Contracts of issues that become apparent.
Rec. 9-11 (#8)		Develop communication plans for contracts that identify roles and responsibilities of agency and vendor representatives, as well as how and when they communicate					**OCIO July 2019:** This is the responsibility of individual agencies depending on the way roles and responsibilities are defined in their contracts. **August 2020:** Ongoing. Communication plans identifying roles and responsibilities for agencies and vendors for ongoing contract maintenance should be part of new contract language and guidance developed in conjunction with DES.	
	Complete		Agency 3	5/2020	Yes	No	No	Communication plans are routinely required as a deliverable in The agency's IT contracts either in the Statement of Work or the RFP. Vendor also participates in Implementation Planning Study Workshops prior to final award of contract.

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
	Complete		Agency 5	5/2020	Yes	No	No	This is ongoing. As each IT contract is developed, these requirements are flushed out.
Rec. 9-11 (#9)		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					**OCIO 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. **August 2020**: Complete. An OCS-facilitated presentation by the DES state risk manager was conducted in July 2019. This presentation included information on cyber liability insurance provided by the state as well as the kind and amount of cyber liability insurance to be carried by the vendor.	
	In Progress		Agency 1	3/2020	Yes	No	No	The agency security team is not currently working with DES ORM or the AGO for contract language. The security team will continue to collaborate with the agency contracting department to ensure that a process is developed to engage with DES ORM and the AGO going forward.
	Complete		Agency 2	3/2020	Yes	No	No	We stay in close coordination with our Agency Risk Manager who is the POC for DES Risk Manager and cyber liability.
	Complete		Agency 3	3/2020	Yes	No	No	The agency's IT Contracts Administrator attended this workshop as well as one provided by the AGO. DOH IT contracts and RFPs have included the requirement for cyber liability since 2016 based upon consultation with and recommendations of the DES Risk Manager

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
	Complete		Agency 4	3/2020	Yes	No	No	
	Complete		Agency 5	3/2020	Yes	No	No	We carry cyber liability insurance and incorporate an appropriate level of insurance in contracts
Rec. 9-11 (#10)		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					**OCIO July 2019:** OCS has begun discussions with DES contracts to uniformly define what the term "immediately" means. This will provide consistent instruction to vendors as to when security breaches and incidents should be reported to the agency. **August 2020:** Work was suspended on this pending passage of Substitute House Bill 1071, which updated the state's breach notification laws. The updated law retains the language that vendors must "immediately" notify in the event of a breach. As this is a legal term codified in statute, OCS will work with the Office of the Attorney General, the State Privacy Officer and DES to determine whether a uniform time period (e.g. "24 hours") can be used in all vendor contracts as a means of interpreting "immediately".	
	In Progress		Agency 1	7/2019	Yes	No	No	The agency will use the guidance from OCS and DES on the interpretation of the word "immediately".
	Complete		Agency 2	7/2019	Yes	No	No	We have defined notification timelines from vendors based on the sensitivity (CAT1-4) and business impact of data stored or processed by the vendor. 24-72 hours timeline.
	Complete		Agency 3	7/2019	Yes	No	No	The agency's standard contract templates provide for notification of actual or suspected breach within 1 business day based on advice from DOH Security Officer. DOH is awaiting the outcome of the OCS/DES discussion(s). DOH has

Issue/ Rec	Status	Action Steps	Lead Agency	Due Date	Current Resources ?	Budget Impact ?	Legislation Required?	Notes
								implemented interim definition to mean one (1) business day and will determine if an adjustment is needed once we receive further instructions from DES/OCS.
	Complete		Agency 4	7/2019	Yes	No	No	
	In Progress		Agency 5	7/2019	Yes	No	No	Will follow what OCS and DES determine.
Rec. 9-11 (#11)		Agency 3 and agency 5 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					**OCIO 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. **August 2020:** Complete. OCS, a part of its security design review function, works with agencies and vendors to provide guidance when vendors provide "commodity" click-through services that do not comply with IT security requirements, and provide recommendations as to whether these services should or should not be implemented based on the risk associated with use of the service.	
			Agency 3	3/2020	Yes	No	No	The agency is looking for OCIO to lead this change.
	Complete		Agency 5	3/2020	Yes	No	No	We no longer conduct business with vendors who cannot meet the IT security standards.