WaTech
Washington Technology Solutions

1500 Jefferson Street SE | Olympia, WA 98504-1501
watech.wa.gov

Official Response to the Performance Audit on Controls to Manage Outdated Applications September 1, 2023

This management response to the State Auditor's Office (SAO) performance audit report received on August 7, 2023, is coordinated by the Office of the Chief Information Officer (OCIO) on behalf of the audited entities.

SAO Performance Audit Objectives:

The SAO looked at three state agencies to see if they have procedures to identify legacy applications and address their risks through these three questions:

1. Are there opportunities to improve their processes for identifying and monitoring the use and maintenance of legacy applications?
2. Do they assess risks for legacy applications to ensure they are appropriately secured, and support their business mission and objectives?
3. Do they have a strategy (or take corrective actions) to mitigate the risks identified for their legacy applications?

SAO Recommendations 1-3 to the selected state agencies:

To better identify and track legacy applications:

1. Develop and implement a policy or process to identify and track legacy applications.
2. Update and review their information technology (IT) application inventory data to ensure it is complete and accurate.
3. Develop and implement a process to calculate and monitor the maintenance cost for each IT application, including internal/in-house costs and vendor expenses.

STATE RESPONSE

Agency A:

Concur. Agency A will align IT Standards to the new IT organizational architectural model. The agency will adopt the OCIO definition of legacy applications, and they will be tracked in the Applications Portfolio. The Application inventory will be reviewed at least annually, and the agency will continue to update and review inventory data to ensure it is complete and accurate. The agency will continue to track and monitor implementation and maintenance cost with the usage of project type fields in AFRS to represent Acquisition/Development and Maintenance and Operations per SAAM and OCIO. This data will continue to be provided to OCIO for entry into the state IT Financial Management system.

Agency B:

Concur. Agency B has developed and implemented policy and process to identify and track legacy applications. The Application Inventory has been improved by updating missing information identified in the audit. We are also working to calculate and monitor the maintenance cost for each IT application, including internal/in-house costs and vendor expenses.

Agency C:
Concur. Agency C will work with the OCIO to provide input, review, and then implement a policy that defines/identifies legacy applications. Once defined, we will develop requirements, modify, test, and implement changes to our existing application portfolio cataloging system to incorporate the new OCIO policy on legacy applications. Next, we would work with our customers to prioritize the research and data gathering needed to populate the newly created fields related to legacy applications for each application within our application portfolio cataloging system.

Action Steps and Time Frame

Agency	Action Step	Due Date
Agency A	Align IT Standards to new IT organizational architectural model. Track application in the Applications Portfolio.	December. 31, 2023
	Coordinate review of IT Application inventory at least annually.	September 30, 2023
	Track and monitor implementation and maintenance costs with the usage of project type fields in AFRS and provide this data to OCIO.	September. 1, 2023
Agency B	Develop and implement policy and process to identify and track legacy applications.	
	Complete the IT application inventory data and review it for accuracy.	December. 31, 2023.
	Calculate and monitor the maintenance cost for 25% of the agency's IT applications.	March 31, 2024
	Calculate and monitor the maintenance cost for all IT applications.	March 31, 2025
Agency C	Develop and implement a policy that defines/identifies legacy applications.	September. 30, 2024
	Update our existing application portfolio to incorporate the OCIO policy on legacy applications.	July 30, 2025
	Work with customers to prioritize populating new fields in our application portfolio cataloging system.	December. 31, 2025

SAO Recommendations 4-6 to the selected state agencies:

To improve IT application risk and security assessment processes, as described on pages 20-25, we recommend the agencies:

4. Develop and implement a policy or process to perform both IT application risk and security assessments that is consistent with standards issued by the Office of the Chief Information Officer (OCIO)
5. Perform periodic IT risk and security assessments on all IT applications.
6. Establish formal vulnerability management procedures. Documentation should include:
   - What assessments were performed for the identified vulnerabilities.

- How the vulnerabilities were prioritized
- The actions taken to mitigate the vulnerabilities or the reasons for not taking any actions.
- How to verify the mitigations

STATE RESPONSE:

Agency A:

Concur. Agency A will draft, publish, communicate, and implement a policy for conducting application risk and security assessments consistent with OCIO standards. The agency will also develop, publish, communicate, and implement formal vulnerability management procedures.

Agency B:

Concur. Agency B is working on a policy and process to perform both IT application risk and security assessments that are consistent with standards issued by the OCIO. The agency will also perform routine IT risk and security assessments once policy and procedures are in place. Agency B will also update policy and procedures to address vulnerability management procedures as recommended in the audit.

Agency C:

Concur. Agency C will build on current policies and practices to ensure its IT application risk and security assessments, and vulnerability management processes are consistent with standards established by the OCIO. The agency has also been working to enhance its Cybersecurity Risk Management program and is currently assessing tools and processes related to cybersecurity risk and security assessments.

Action Steps and Time Frame

Agency	Action Step	Due Date
Agency A	Complete policy for conducting application risk and security assessment.	August 1, 2024
	Set a timetable for Periodic IT risk and security assessments on IT applications	August. 1, 2024
	Complete procedures for management vulnerability.	August. 1, 2024
Agency B	Complete application risk and security policies and procedures.	December 31, 2023
	Perform a risk assessment on one priority application and, going forward, conduct risk assessments on new applications prior to implementation.	December 31, 2023
	Establish a risk and security assessment schedule for all remaining applications.	December 31, 2023
	Establish vulnerability management procedures in keeping with audit recommendations.	March 31, 2024

1500 Jefferson Street SE | Olympia, WA 98504-1501
watech.wa.gov

Agency	Action Step	Due Date
Agency C	Review and update internal policies to ensure risk and security assessments are consistent with the OCIO's recently updated risk and assessment standards.	March 31, 2024
	Identify and schedule system assessments consistent with the OCIO's recently updated risk and security assessment standards.	March 31, 2024
	Modernize vulnerability management system and procedures, including addressing the items identified in the audit report.	May 31, 2024

SAO Recommendations 7-8 to the selected state agencies:

To choose the best application modernization option with the highest effect and value, as described on pages 26-28, we recommend the agencies:

7. Improve their modernization decision-making process by conducting qualitative and quantitative analyses on the available options, including:
   - Cost-benefit or return-on-investment analyses
   - Analyses demonstrating how the agency prioritized the options.
8. Maintain documentation supporting their decision for modernization options.

STATE RESPONSE:

Agency A:

Concur. Agency A has implemented an IT modernization strategy work group to address improving modernization decision making processes. The Agency is currently undergoing an upgrade with the existing portfolio software vendor that will facilitate modernization decision tracking for the agency. As we look to modernize our applications, funding and resources continue to be a challenge.

Agency B:

Concur. Agency B has incorporated the modernization decision-making process and all related approvals and analysis completed into our governance structure. Going forward, we will conduct qualitative and quantitative analyses, as recommended, within our decision-making processes. The agency also now maintains documentation supporting decisions for modernization options.

Agency C:

Concur. Agency C will build on the work of its internal technology governance for prioritizing IT projects. This includes identifying options to mitigate risks associated with agency applications and incorporating cost-benefit metrics for decisions on modernizing applications. Minutes from meetings will be documented appropriately.

Action Steps and Time Frame

Agency	Action Step	Due Date
Agency A	Implement an IT Modernization Strategy Work Group. Upgrade existing portfolio software to facilitate modernization decision tracking.	August 22, 2024 September 30, 2023
Agency B	Not applicable.	
Agency C	Establish a process to identify application risks and mitigation options to bring forward to the appropriate level within the agency. Identify the best option of incorporating application cost-benefit metrics related to modernization. Develop and implement a technology-based solution that will provide access to minutes and decisions for internal stakeholders on additional metrics related to application modernization.	June 30, 2024 June 30, 2024 December 31, 2024

SAO Recommendations 9-10 to the Office of the Chief Information Officer (OCIO):

To help state agencies better identify and track legacy applications to be replaced or upgraded, as described on pages 13, 14 and 18, we recommend the OCIO:

9. Develop and implement a statewide standard and policy to identify and track legacy applications.
10. Implement a policy and process, such as a required periodic review of IT application inventory data, to ensure statewide application inventory records are complete and accurate.

STATE RESPONSE:

WaTech concurs with the report's findings and recommendations. However, WaTech believes the basis of these recommendations have been met through existing guidance and recently adopted improvements to the OCIO standards.

On page 13 of the audit report, SAO provides guidance from our FY20-21 IT Biennial Report identifying "Legacy Applications." Additionally, page 35 classifies an application as "Old" if the application has been in use for 15 years or more. While these factors are important to determine whether an application should be modernized; the " legacy " issue is much more complex than just the age of an application.

Further, OCIO policy 112, adopted by the TSB on March 10, 2020, requires:

"Each agency must establish processes to collect the foundational set of portfolio inventory elements and update this information on at least an annual basis:

a. Agency applications.

i. Standard 112.10 defines the minimum set of data to be collected on application and information systems."

1500 Jefferson Street SE | Olympia, WA 98504-1501
watech.wa.gov

WaTech recently updated the guidance for determining application legacy and whether one should be modernized. In June 2023, the Technology Services Board (TSB) approved application policy standard 112.10 updates — now referred to as MGMT-01-01-S. This standard includes an updated Application and Infrastructure Inventory Template. The new template contains 49 fields related to all agency applications. Agencies must track and submit this information to WaTech annually. Ten of these fields relate to application legacy and modernization. Five of these questions relate to application quality, and the remaining relate to the value of the application to the business. Responses to these ten questions determine whether a given application is "legacy." This new guidance appears in Technology Standard MGMT-01-01-S Technology Portfolio Foundations – Applications, including:

Question	Guidance	
Does the application constrain a business process or service?	If the application is a constraint to improving a business process or service and/or presents a business or operational risk to the organization, the answer is yes	Business Value
Is on an aging technology	Review the list of key technologies and select which applies. If multiple dropdown options of less modern key technologies apply, please select the most prominent. Access / Adabas C / Classic ASP Cobol / DB2 Delphi / Fortran Fox Pro / IBM PL/1 Pascal / PERL Sybase New 4 / VBA VB.NET / No - key technology not on this list	Application Quality
Is on an unsupported version	If the application is running on unsupported version of technology.	Application Quality
Is updatable	If the application has all resources to update, the answer is Yes.	Application Quality
Mainframe application	If applicable, list the mainframe service. • State enterprise mainframe (on the state shared service mainframe). • Agency mainframe (On agency managed mainframe and not on the state enterprise shared service mainframe). • Other mainframe (On a mainframe that is not managed by the agency and not on the state enterprise shared service mainframe).	Application Quality
Has resources available	If all required resources are available to run/support the application, the answer is Yes.	Application Quality

Question	Guidance	
Business owner	Item owner or person responsible for this item.	Business Value
Business Criticality	Agency self-defines application criticality to the organization. • Business Essential (If unavailable there is direct negative customer satisfaction; compliance violation; non-public damage to organization's reputation; direct revenues impact). • Historical (Needed for historical purposes). • Mission Critical (If unavailable there is widespread business stoppage with significant revenue or organizational impact; Risk to human health/environment; Public, wide-spread damage to organizations reputation)/ • User Productivity (If unavailable there is impact to employee productivity.	Business Value
Has other risks	If the agency has identified other risks related to security, vendor support or contract management, the answer is Yes.	Business Value
Mobile	Identify if this application is intended to deploy to a small-format mobile device like a tablet or smartphone. Some web applications may have been built with adaptive or responsive design web technology that allows the content to scale/display on tablets or smartphones – those should be considered mobile application).	Business Value

These elements are used to apply Gartner's Application TIME model. TIME is an acronym for Tolerate (High-quality application/low business value), Invest (High-quality application/high business value), Migrate (Low-quality application/high business value), or Eliminate (Low-quality application/low business value). This quadrant chart provides a visual analysis tool for / where an agency should invest its efforts to improve its application portfolio.

WaTech believes that this policy and procedure meet the foundation of SAO's recommendation: "develop and implement a statewide standard and policy to identify and track legacy applications." Therefore, while WaTech continually works with stakeholders to keep up with the changing IT landscape, it has no definitive plans to change the existing processes. However, these procedures and criteria are evaluated annually, and other elements may be added in the future to further define "legacy applications."

Regarding the SAO's recommendation to require periodic reviews of IT application inventory, agencies are already required to provide WaTech with information about their application inventories every year as noted above. WaTech examines these responses and follows up with agencies multiple times to discuss the inventory information's accuracy when it is incomplete.

Action Steps and Time Frame

Not applicable.