PERFORMANCE AUDIT

Office of the Washington State Auditor
Pat McCarthy

Controls to Manage Outdated Computer Applications

September 5, 2023

Report Number: 1033149

Table of Contents

State Auditor's Office contacts

State Auditor Pat McCarthy
564-999-0801, Pat.McCarthy@sao.wa.gov

Scott Frank – Director of Performance and IT Audit
564-999-0809, Scott.Frank@sao.wa.gov

Peg Bodin – Assistant Director for IT Audit
564-999-0965, Peggy.Bodin@sao.wa.gov

Justin Stowe – Assistant Director for Performance Audit
564-201-2970, Justin.Stowe@sao.wa.gov

Shauna Good – Principal Performance Auditor
564-999-0825, Shauna.Good@sao.wa.gov

Karen Wilson – IT Systems Program Manager
509-581-3990, Karen.Wilson@sao.wa.gov

Audit Team: Won Cho, Jon Howard

Kathleen Cooper – Director of Communications
564-999-0800, Kathleen.Cooper@sao.wa.gov

To request public records

Public Records Officer
564-999-0918, PublicRecords@sao.wa.gov

Americans with Disabilities

In accordance with the Americans with Disabilities Act, this document will be made available in alternative formats. Please email Webmaster@sao.wa.gov for more information.

Executive Summary

State Auditor's Conclusions (page 29)

A thread throughout this performance audit is a simple idea – that Washington's state agencies should have a uniform and consistent approach to identifying legacy applications. Supporting that work with a statewide policy will be complex, but nonetheless important.

Legacy applications are more vulnerable to security threats, decreased performance and expensive maintenance. However, by their very nature, such applications vary as widely in their purpose and design as state agencies do in their core missions. Agencies may not have a definition of a legacy application. Nonetheless, developing a definition will help them consistently identify applications whose age, risks and costs warrant the expense of replacement.

After reviewing the efforts of three state agencies, this audit makes several recommendations to develop a more uniform approach to identifying and tracking legacy applications, assess risks associated with those applications, and perform sufficient analyses of modernization options. In this effort, there is also a role for the state's Office of the Chief Information Officer to implement a statewide standard and policy for legacy applications.

Through these recommendations, state agencies can better track legacy applications, address the risks they present and plan for their ultimate replacement, which will help the state limit risk and deliver more effective service to Washingtonians in the long run.

Background (page 7)

Washington's governments use information technology (IT) applications every day to perform many critical functions, from supporting public safety and providing social services to collecting taxes and managing public transportation. Each application has a lifespan, and those used beyond the point where they might be retired are frequently called "legacy applications." These products use outdated technology, are often incompatible with more modern IT systems, and are challenging to maintain.

Washington Technology Solutions, the state's centralized provider and procurer of IT services, estimates that between 40 percent and 60 percent of the state's government applications should be considered legacy. State agencies that

use legacy applications face many risks, which could include greater security threats, decreased performance and expensive maintenance. For example, legacy applications are more vulnerable to cyberattacks when they are incompatible with modern security features. They are also slow, inefficient and more likely to fail, which can affect a government's ability to achieve its objectives. In addition, the long-term costs of maintaining legacy systems can outweigh the trouble and expense of transitioning to new software.

This audit looked at three state agencies to see if they have procedures to identify legacy applications and address risks associated with them.

Agencies could better manage IT risks by defining what constitutes a legacy application, keeping accurate and complete application inventory records, and monitoring maintenance costs (page 12)

Establishing criteria for what constitutes a legacy application could help agencies identify legacy applications consistently. However, audited agencies lacked policies or guidelines that established criteria for a legacy application. Statewide policy or guidance could help agencies define and identify legacy applications.

In addition to these criteria, maintaining accurate and complete IT application inventories is critical for managing software assets, because it helps management make informed decisions. We found agencies' IT application inventory records were incomplete and contained inaccurate information, largely due to insufficient staffing, competing priorities and a lack of oversight. Incomplete and inaccurate inventories limit management's ability to make informed decisions, and they affect the accuracy of statewide inventory records.

As part of tracking and monitoring IT applications, collecting complete and accurate information on their maintenance costs can also help management make informed decisions about the cost-effectiveness of applications needed to support operations. We found agencies did not periodically identify, calculate, or monitor the maintenance cost for each IT application accurately and completely, because they did not prioritize resources for monitoring maintenance costs due to competing demands for limited resources.

Agencies were inconsistent in conducting periodic risk and security assessments on IT applications

(page 20)

Washington's Office of the Chief Information Officer (OCIO) requires state agencies to conduct two types of application assessments – risk and security – which help them identify potential problems relating to application security and business objectives. We found two agencies did not perform formal risk assessments on applications. While the third agency does conduct some formal risk assessments, it could improve its process by following state requirements.

We also found all three agencies periodically conducted state-required security assessments on IT devices and infrastructure, but not on applications. They also did not routinely document how they manage vulnerabilities. These gaps between OCIO standards and agency assessments were due to a misunderstanding of the full requirements, insufficient staffing and competing priorities. Ultimately, our review of agencies' own vulnerability scanning of servers identified potential security issues for their applications.

Agencies could use qualitative and quantitative analysis to help them choose the best modernization option (page 26)

Leading practices advise performing both qualitative and quantitative analyses to identify options available to mitigate the risks associated with legacy applications. As part of the audit, we reviewed six IT modernization projects – two for each of the audited agencies – to see how each agency had arrived at its decisions. We found only one project where an agency had sufficiently analyzed all available options for modernization. Washington agencies could improve their decision-making process for choosing modernization options by conducting sufficient analyses and recording them.

Recommendations (page 30)

We made a series of recommendations to the three audited state agencies to better identify legacy applications and address risks associated with them. For example, we recommended that agencies develop a policy or process to identify and track legacy applications, and perform both application risk and security assessments that align with state requirements.

We also recommended that agencies improve their application modernization decision process by performing sufficient analyses and recording them. We further recommended the OCIO help agencies better identify and track legacy applications by implementing a statewide standard and policy.

We also suggested all Washington state agencies consider the recommendations made to the audited agencies as they develop and implement their controls to manage legacy applications.

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 Office of the State Auditor 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 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

Washington relies on smoothly functioning IT applications to perform a host of critical governmental functions

An information technology (IT) application is a computer program designed to carry out a specific task for people who use it. Its purposes are more specific than the operating system software that makes computer hardware run; typical applications include word processors, media players and accounting software. Governments large and small, state and local, use applications to perform a variety of critical functions, supporting public safety, social services, tax collection and transportation. Some applications are common in both public- and private-sector offices; many in government are specialized, even custom-made, to serve purposes that are unique to individual agencies. Government operations – and the safety and well-being of the state and its residents – rely on those applications to be stable, secure and ready to use whenever they are needed.

IT specialists assess an agency's software performance through life cycle analyses

IT staff or consultants are typically responsible for managing software throughout its life cycle to ensure it serves its intended purpose until it is no longer needed or suitable. The life cycle management steps – illustrated in **Exhibit 1** and described below – are typical for a government organization that may purchase or commission some software but is capable of developing applications for some of its specialized needs.

Exhibit 1 – IT application life cycle stages

1. Identify what users need the application to do. Before buying or developing a new application, designated project leads (IT staff and others in the government) gather information to understand what users want the application to do to support their work. Defining application requirements takes many elements into account, such as compliance requirements and the number of users and their locations.

2. Decide whether to buy or develop. After defining requirements, project leads decide whether to purchase a commercial, off-the-shelf applications – which include options such as Software as a Service (SaaS) and Platform as a Service (PaaS) – or build a custom one. They evaluate multiple factors, such as whether the organization's internal IT division can build the application, whether commercial software could meet user needs, and the costs and benefits of each option.

3. Install and roll out the application to users. This step may also involve testing and training after IT staff install the new software and set up necessary permissions on every computer or system using it.

4. Maintain the application. IT staff monitor and manage the application's performance. They resolve any issues while also evaluating its security.

5. Monitor and assess regularly for planned retirement. An important element of the maintenance stage is deciding when maintenance activity should stop and the organization upgrade to a newer version of the product or migrate to a different one.

"Legacy applications" are the stopgap of maintaining a product past the point where it might be retired

The final step on the life cycle path may be extended if the application continues in service after reaching its end of life. So-called "legacy applications" use outdated technology, are often incompatible with more modern IT systems, and have become challenging to maintain. To determine when a software should be deemed a legacy application, an organization must consider many issues, including:

- **Security:** It runs on obsolete technology, is overexposed to security vulnerabilities and cannot be updated to meet modern cybersecurity standards.
- **Performance:** It is too slow to process current volumes of data efficiently, has more downtime, or does not meet evolving organizational needs.
- **Compliance:** It no longer meets evolving standards of compliance regulations.
- **Support:** A developer or vendor no longer provides support, maintenance or updates for it.
- **Maintenance cost:** Maintenance costs to support the application become increasingly high.

Legacy applications can increase security risks, hinder an organization's ability to deliver its mission, and increase maintenance costs

Legacy applications can pose three significant problems for government organizations: greater security risks, decreased performance and expensive maintenance.

Legacy applications are more vulnerable to cyberattacks when they are incompatible with modern security features. In one example, the U.S. Office of Personnel Management experienced a security breach due in part to its reliance on legacy applications, which it had difficulty upgrading and encrypting. This June 2015 breach affected 22.1 million records, including records related to government employees, other people who had undergone background checks, and those friends and family listed as references.

These applications are comparatively poor performers. Since they are slow, inefficient and more likely to fail, they may not appropriately support the organization's objectives, especially under pressured circumstances. For example, when the COVID-19 pandemic prompted a surge in unemployment claims, both Wisconsin's and Vermont's outdated unemployment insurance systems repeatedly froze and crashed, preventing staff from processing people's claims promptly and accurately. Both states experienced significant payment delays and a higher rate of incorrect claim denials that could be attributed to failures in the legacy applications.

Finally, maintaining legacy systems can cost an organization more in the long run than the trouble and expense of transitioning to new software. For one thing, it becomes increasingly difficult to find IT professionals with adequate knowledge to keep largely outdated technology operational, and hiring these experts comes at a price. As the number of bugs or glitches to be fixed grows, the long-term costs of maintaining the application compound, too. These costs can outweigh the benefits of maintaining the application. According to the federal Office of Management and Budget and the U.S. Government Accountability Office, in fiscal year 2020, the federal government spent nearly $90 billion on IT investments and operations. Legacy IT maintenance costs accounted for one-third, about $29 billion, of that total spending.

Other audits in the U.S. identified legacy application risks

Audits conducted by other governments over their own legacy applications identified similar risks in managing them. For example, a 2018 audit found the U.S. National Archives and Records Administration lacked adequate controls to identify

and monitor its use and maintenance of legacy IT systems. Among the problems, the Administration did not:

- Establish criteria to identify legacy systems
- Document the age of its systems
- Know the true cost of all its systems
- Have a centralized process to track legacy systems
- Conduct risk assessments for all its information systems

As a result, the audit found the Administration could not ensure information security protections were in place commensurate with the risk to the confidentiality, integrity and availability of its information systems.

In addition, a 2019 audit at the U.S. Department of Energy found it lacked a plan to identify and replace legacy systems. The department had not defined what constituted a "legacy system," and lacked a comprehensive plan to reduce or eliminate legacy IT systems across its operations.

Finally, a 2020 audit of city systems in San Diego found similar issues. The city had not defined what characteristics qualified a system as "legacy." Furthermore, the city's application inventory was missing critical information about the applications – such as a legacy system indicator, accurate system age and expected lifespan – that would have allowed IT staff to assess the applications' viability and possible risks to city operations. Additionally, the city did not centrally track the full cost of its legacy systems, so it could not perform return-on-investment calculations to help staff justify and prioritize application replacements.

Many Washington state agencies face similar legacy application risks

According to a 2014 report issued by the OCIO, Washington is not immune to the risks posed by legacy applications and IT systems. It noted that of the 1,983 total state IT applications reported, 619 (31 percent) were legacy applications that were not fully meeting the evolving needs of the agencies using them. The study determined an application was "legacy" if it did not fully meet business needs for one or more of the following reasons:

- It was not easy to update.
- It was costly to maintain or modify.
- It depended on other unsupported underlying software.
- It had other risks, such as vendor instability, or did not work well with other IT systems.

Washington Technology Solutions (WaTech), the state's centralized provider and procurer of IT services, estimates that between 40 percent and 60 percent of Washington government applications should be considered legacy. On the list were numerous central applications used by almost all state agencies, including the Agency Financial Reporting System and the Human Resources Management System. Both applications are being modernized as part of the OneWashington project.

This audit evaluated selected state agencies' controls for IT application life cycles to mitigate the risks related to legacy applications

This audit looked at three state agencies to see if they have procedures to identify legacy applications and address risks associated with them. The audit was designed to answer the following 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?

Audit Results

Note on reporting protected information

To protect the agencies' information technology (IT) applications, and the confidential and sensitive information contained in them, this report does not include the agencies' names or the detailed descriptions of our results. This information is exempt from public disclosure in accordance with RCW 42.56.420(4). We shared detailed results with each of the audited agencies and with Washington Technology Solutions (WaTech).

Agencies could better manage IT risks by defining what constitutes a legacy application, keeping accurate and complete application inventory records, and monitoring maintenance costs

Results in brief

Establishing criteria for what constitutes a legacy application could help agencies identify legacy applications consistently. However, we found audited agencies lacked policies or guidelines that established criteria for what constitutes a legacy application. A statewide policy or other guidance could help agencies define and identify legacy applications. In addition to defining what is a legacy application, maintaining accurate and complete IT application inventories is a critical part of managing software assets, because it can help management make informed decisions.

We found agencies' IT application inventory records were incomplete and contained inaccurate information, largely due to insufficient staffing, competing priorities and a lack of oversight. Incomplete and inaccurate inventory records ultimately affect the accuracy of statewide inventory records. As part of tracking and monitoring IT applications, collecting information on maintenance costs can also help management make informed decisions. We found all three agencies did not periodically identify, calculate, or monitor the maintenance cost for each IT application accurately and completely, because they did not prioritize resources for monitoring maintenance costs due to competing demands for limited resources.

Establishing criteria for what constitutes a legacy application could help agencies identify them consistently

For a government agency to effectively manage the risks legacy applications pose to security, efficiency and costs, it must first recognize which applications are possible problems. A reasonable first step in identifying such applications consistently is to develop clear criteria to describe "legacy," and document the criteria in a policy or procedure so all IT staff evaluate applications to the same standard.

As they develop their own criteria, a useful starting point for Washington agencies is the definition of a legacy application offered in the FY20-21 IT Biennial Report, which provides an overview of the state's IT landscape, issued by the Office of the Chief Information Officer (OCIO) at WaTech. The OCIO uses this definition (shown in **Exhibit 2**) to identify legacy applications from the statewide application portfolio inventory data.

Exhibit 2 – OCIO's statement setting out "WHAT IS A LEGACY APPLICATION?"

- The system cannot be easily updated due to complicated or unclear code, fragile interfaces, or lack of documentation.
- Maintenance or modification of the system depends on expertise that is hard to find or prohibitively expensive.
- The system depends on software no longer supported by the vendor.
- Other risks identified by agencies, such as vendor instability and lack of alignment with enterprise architecture or a lack of in-house expertise.

Source: FY20-21 IT Biennial Report, issued by WaTech's OCIO.

These defining characteristics have not been formalized or incorporated into statewide standards or policies, but agencies could use them in their own policies regarding legacy applications.

Audited agencies lacked policies or guidelines that established criteria for a legacy application

Agency staff and managers we interviewed said they considered their current application governance procedure sufficient for monitoring application life cycles. However, each technical owner we interviewed held a different view of what constituted a legacy application – and these views were inconsistent even within the same agency.

For example, one said that an application could be considered legacy if it was "aged 10 or 15 years old," built on an outdated platform, or had significant issues. Another technical owner from the same agency would not consider an application to be legacy if it could be updated and supported to achieve its mission, regardless of its age. Because this agency lacks standard criteria to identify a legacy application, staff inconsistently recognize legacy applications and risks associated with them.

Technical term insight

Technical owners are responsible for monitoring and communicating the status and life cycle concerns of agency applications.

Business owners are responsible for the day-to-day use of applications, and best understand users' needs or issues they encounter.

Statewide policy or guidance could help agencies define and identify legacy applications

OCIO has not yet issued a statewide policy or guidance for agencies on how to establish criteria for identifying a legacy application that should be significantly upgraded, retired or replaced. Useful guidance might include descriptions of characteristics to look for, with a model or example agencies could follow to develop their own policies that identify legacy applications.

By developing more consistent criteria for legacy applications, agencies will be more likely to correctly identify such software in their reports to OCIO. As a result, Washington will have a comprehensive and consistent awareness of the extent of legacy applications statewide, which is important to manage overall state IT security and provide a strategic direction for IT governance.

Incomplete and inaccurate IT application inventory records limit management's ability to make informed decisions

Maintaining an accurate and complete IT application inventory is the next essential step in managing software assets. With all applications listed in one inventory, an organization can assess the technical and business value of each one, as well as understand its status. To be complete, inventories should gather metrics, such as an application's age, how it is supported, what technology is used, and its interrelationships with other applications. Organizations can use this data to evaluate and plan whether and when a particular application should be retained, upgraded, retired or replaced.

In Washington, OCIO Policy 112, Technology Portfolio Foundation, requires all state agencies to collect specified information about all applications; it instructs them to also update and report this information to OCIO at least annually. Policy 112 established the 39 application elements that agencies must collect to develop foundational knowledge of their applications. All 39 required fields are essential to accurately assess the application's status. In addition, some fields – such as an application's age, how it is supported, and what operating system and technology are used – can be used to identify a legacy application. The policy is summarized in **Appendix C**.

Agencies' IT application inventory records were incomplete and contained inaccurate information

We reviewed the 2021 and 2022 application inventory data the three audited agencies submitted to OCIO, shown in **Exhibit 3** (on the following page) as A, B and C. Of the three, our review of Agency C found only minor issues. However, for agencies A and B, we found problems in two areas: applications that were not catalogued in the inventory, and key information about catalogued applications that was missing or incorrectly reported. Such errors virtually ensure that the report data reviewed by OCIO is also incomplete.

- **Applications were not catalogued.** Uncatalogued software is much less likely to be tracked for business value, technical issues or support status. At Agency A, we found 12 third-party vendor applications were not catalogued in the inventory.
- **Key information was missing.** At Agency B, we found that all 121 applications in the 2021 inventory lacked data in 16 key fields. The fields represent basic, essential information about the application, including the description, business and technical owners, and more. Additionally, the service start date was missing for 55 applications. Five fields that can be used to identify a legacy application, including service start date (indicating an application's age), operating system and key technologies, lacked data. Old applications that run on obsolete technologies and operating systems could be overexposed to security vulnerabilities and more challenging to maintain, so they could be categorized as a legacy. Agency B made an improvement in collecting data for the 2022 application inventory, but four key fields – description, business and technical owners, and in-service date – were missing for multiple applications.

  At Agency A, the 2021 inventory was more complete, but nonetheless lacked data in four key fields for all 26 applications used by the agency. The 2022 inventory data lacked data in the same fields for all 34 applications in use that year. That year, another nine key fields lacked data for multiple applications, some of which can be used to identify a legacy application.

Exhibit 3 – Number of applications without key information in agency inventories

Selected entries from agencies' annual application inventories from 2021 and 2022.
Fields marked ♦ could be used to identify legacy applications.

	Agency A		Agency B		Agency C	
Missing data in these fields	***2021***	***2022***	***2021***	***2022***	***2021***	***2022***
Description			121	55		
Technical owners		1	121	51		
Business owners		1	121	49		
Date acquired			121			
Manufacturer/Vendor			121			
Cloud service provider			121			
Source supplier			121			
Contract number			121			
License number			121			
Version information			121			
♦ Operating system	4	4	121			
♦ Operating system version	4	4	121			
♦ Authentication type	1	1	121			
♦ Key technologies	26	34	121			
Database relationship	26	34	121			
Relationships to other infrastructure	26	34	121			
Relationships to other applications	26	34				
♦ In-service date		3	55	63		
Business criticality		1				
♦ Is updatable		1				
Life cycle		2				
♦ Has resources available		2				
♦ Is running on an unsupported version		2				
♦ Has other risks		4				
Total number of applications that should have had data	*26*	*34*	*121*	*170*	*499*	*564*
Number of applications missing at least 1 data field	**26**	**34**	**121**	**63**	**0**	**0**

Source: Auditor analysis of application inventories supplied by audited agencies.

- **Inaccurate data can be as problematic as missing data.** Even though Agency A reported application data in most required fields, the data in nine fields was incorrect or, at the least, misleading. For example, as **Exhibit 4** shows, the business owner and technical owner were not properly identified for most applications.

Exhibit 4 – Agency A's applications inventory had numerous incorrect attributions
Selected entries from Agency A's annual application inventories from 2021 and 2022.

	Agency A	
Incorrect data in these fields	***2021***	***2022***
Description	1	1
Technical owners	25	26
Business owners	24	26
Core business function	2	2
Used across government	1	1
Integrates with federal systems	2	2
Total number of applications that should have had correct data	*26*	*34*
Number of applications with at least one incorrect field	**25**	**26**

Source: Auditor analysis of application inventories supplied by audited agencies.

As noted in the sidebar on page 14, "technical owner" employees are responsible for day-to-day use of the application and managing its technical aspects. They are also responsible for entering inventory data for their assigned applications. However, for these applications, the business owner listed was the agency's assistant secretary or agency. This role is an executive-level position, making high-level decisions around overall operations and not in practice responsible for applications on the business side. The listed technical owner was the IT director; again, a role less likely to be hands-on responsible for the application. Data was also incorrectly reported in seven other key fields for multiple applications.

Incomplete and inaccurate records were due to insufficient staffing, competing priorities and a lack of oversight

Managers at Agency B said that its IT division had been short-staffed and overburdened with mission-critical projects that had to take priority for several years. Notwithstanding other issues, managers at agencies A and B said limited resources were prioritized on other critical requirements and they did not consider the application inventory a high priority; none made a point of ensuring data was reviewed for completeness and accuracy.

Statewide application inventory records are also incomplete

The incomplete record issue was not limited to the two agencies. During the scoping phase for this audit, we reviewed data in the 2020 statewide application inventory to identify agencies that had a higher percentage of old applications with in-service dates earlier than 2006. This inventory covers all state agencies. While this was only a limited review of statewide data, we found:

- Service start date information was missing for 2,539 out of the total 5,904 applications – 43 percent of all applications
- Life cycle information was missing for 500 applications (8 percent)
- Business criticality information was missing for 552 applications (9 percent)

These missing records indicated that the statewide application inventory was incomplete.

Incomplete and inaccurate information on IT application maintenance costs also limits management's ability to make informed decisions

Application maintenance is an ongoing process of correcting faults in programs and enhancing their performance to keep up with the organization's needs. Accurately identifying and calculating the costs of doing so is an essential step in assessing the application's cost-effectiveness. If expenditures are higher than anticipated, the organization must assess the application to determine whether it is economical to keep in service and should be retired and replaced. By not monitoring a legacy application's maintenance costs, an organization might overlook possible savings by not replacing it with a modern, cheaper and more effective one.

Agencies did not periodically identify, calculate, or monitor the maintenance cost for each IT application accurately and completely

Agencies A and B lacked policies and procedures setting out how staff should identify, calculate and monitor IT applications' maintenance costs. Neither could demonstrate that they could identify application maintenance costs accurately and completely. They did partially track costs for contractor-supported products

by identifying and monitoring spending on the vendors, but did not identify or monitor other maintenance cost components, such as the agency's internal support for these products.

Agency C had developed an internal procedure that spelled out how staff should identify and calculate application maintenance costs, and enter the data in the agency's application inventory record. However, even though the procedure specified updating and reviewing maintenance costs annually, records showed that staff had not reviewed and updated costs annually for seven applications for more than three years. The agency had accounted for the expense of both vendor maintenance and its own internal maintenance. For the internal maintenance portion, the agency calculated the maintenance cost by tracking actual hours spent on maintenance work and applying the hourly rate for IT support staff.

None of the agencies prioritized resources for monitoring maintenance costs due to competing demands for limited resources

Managers at all three agencies said they did not prioritize identifying and monitoring maintenance costs over other IT tasks. A manager at Agency C said monitoring was not prioritized because it was not required to be reported to OCIO.

Agencies were inconsistent in conducting periodic risk and security assessments on IT applications

Results in brief

Washington's OCIO requires state agencies to conduct two types of application assessments – risk and security – which can help them identify potential problems relating to application security and business objectives. We found two audited agencies did not perform formal risk assessments on applications, and the third agency could improve its process by following state risk assessment requirements. We also found all three agencies periodically conducted state-required security assessments on IT devices and infrastructure, but not on applications. They also did not routinely document how they manage vulnerabilities. These gaps between OCIO standards and agency assessments were due to a misunderstanding of the full requirements, insufficient staffing and competing priorities. Ultimately, our review of agencies' own vulnerability scanning of servers identified potential security issues for their applications.

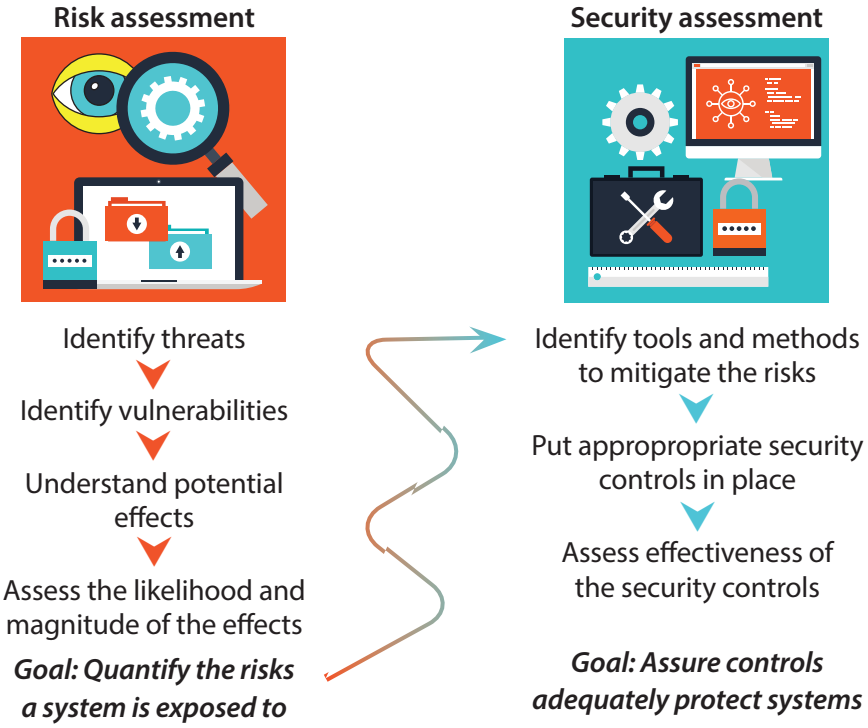
Performing two types of application assessments – risk and security – can help agencies identify potential problems relating to application security and business objectives

Leading practices recommend organizations assess all applications they use against two standards to identify and respond to possible threats to, and vulnerabilities in, their applications.

The first – *a risk assessment* – sets out to identify problems in the application itself to ensure it is appropriately secured and supports an organization's business mission and objectives. Part of this assessment includes determining the likelihood an attack would be successful, as well as how damaging the effect a successful attack would be on operations or data. With this information, agencies can understand the security risks associated with all their applications, particularly those with potential problems that could hinder their ability to deliver their mission.

The second – *a security assessment* – focuses on the tools and methods in place, known as security controls, and how well they function to prevent or minimize the consequences of a successful attack. **Exhibit 5** illustrates how the two assessments work together to illuminate the risks in the applications and the effectiveness of security controls.

Exhibit 5 – Relationship between risk and security assessments



By failing to conduct these two types of assessments, organizations miss a significant opportunity to identify risks to IT systems through their applications. More importantly, they also miss opportunities to address and mitigate those risks. Furthermore, these two assessments provide strategic information when management considers which applications are still useful or need updating or replacement, and which are too costly in terms of risk to retain. These assessments should be considered essential, because they are a way of identifying risks specifically in legacy applications.

Washington's OCIO requires state agencies to conduct application risk assessments

Since 2017, OCIO's Policy 141.10 has required all agencies to conduct both risk and security assessments whenever they introduce new software or make changes to an existing system. The policy also specifically requires agencies to conduct both assessments on all systems processing confidential data at least once every three years. (See **Appendix D** for summaries of OCIO's risk and security assessment requirements.)

In February 2023, during fieldwork for this audit, OCIO adopted new IT policies associated with the application risk assessment that provide more structured,

detailed guidance for the assessment process. Even more important, the new policies require agencies to conduct risk assessments under these circumstances:

- Annually for information systems agencies deem to be business-essential
- Before sharing confidential data with agencies and/or vendors
- When a security patch is not applied. This change reflects a situation in which an agency might choose to postpone applying a security patch until after adequate testing to ensure it will not affect users or the wider IT environment.

Technical term insight

A *security patch* is an update to software or operating systems that addresses security vulnerabilities within a program or product.

Two audited agencies did not perform formal risk assessments on applications

Agencies B and C did not perform formal IT risk assessments on applications. As a result, they could not effectively and consistently identify and address the risks associated with their applications. This means they also lacked important information that could help management decide which software, including legacy applications, should be retired or replaced.

Agency B developed a policy and procedure for IT risk assessments and mitigation in May 2022. However, agency management did not prioritize implementing them due to competing demands for limited resources, so staff had not performed any application risk assessments.

Staff at Agency C said they considered two types of reviews designed for other purposes acceptable as risk assessments. While these reviews can provide agencies with information that may help them identify potential threats, neither are designed to assess risks. The agency currently lacks a risk assessment process that would meet state standards.

The third audited agency could improve its process by following state risk assessment requirements

Agency A does have some risk assessment processes, but their uses are limited. It has one procedure to assess third-party vendor applications, and a second for applications developed in-house. In both risk assessments, the agency identified threats and vulnerabilities, described the effects, and assessed the likelihood of the effects.

However, Agency A did not perform a periodic risk assessment on all applications. For the third-party vendor applications, the agency assessed only new applications, not existing ones. For in-house applications, the current risk assessments do not consider all potential threats specific to applications because they focus primarily on threats to the agency's overall environment, and then identifies how those threats affect applications. A risk assessment focused on identifying threats specific to applications may identify additional threats.

Agencies periodically conducted state-required security assessments on IT devices and infrastructure, but not on applications

OCIO's Policy 141.10 also directs agencies to establish a framework and schedule for conducting assessments that periodically test the security of "a sampling of agency systems, applications and IT infrastructure." The policy offers examples of tools, such as vulnerability scans and penetration tests (see sidebar). It also specifies that agencies must correct any weaknesses identified, for example, by introducing or strengthening IT security controls.

All three agencies conducted periodic vulnerability scans on devices and infrastructure, such as workstations and servers, connected to their networks. However, the scans were not conducted on IT applications because the scanning tool did not have a function to identify vulnerabilities in them. Additionally, none of the agencies had established procedures specifying how to identify a sample of applications to test.

Agency C also has a penetration test team as part of its IT division. The team conducted penetration tests on applications only when it identified a higher security risk, not on a periodic basis. The team also conducted an annual penetration test on its cardholder data environment to ensure compliance with the Payment Card Industry Data Security Standard.

Technical term insight

Vulnerability scanning tools periodically sweep designated hardware and software for gaps or issues that might allow an attacker to successfully breach an IT system or conduct other harmful activities. Examples of "vulnerabilities" these scans identify include a PC running an unsupported operating system, or a computer that can connect to the internet without any password protection.

Penetration testing is a simulated cyberattack against IT systems to check for exploitable vulnerabilities on those systems.

Agencies did not routinely document how they manage vulnerabilities

As noted earlier, Policy 141.10 requires agencies to correct problems found during security assessments, whether through vulnerability scans or penetration tests. Managers and staff at all three agencies said that when scans identified potential vulnerabilities, their IT security teams analyzed the scan results, prioritized problems for remediation, and came up with mitigation actions. They said most issues were caused by missed updates or patches for servers and Microsoft products, including software, which they mitigated by installing the updates or patches. However, this was an ad hoc process, and staff could not show us documentation of a vulnerability management process. The agencies did not maintain evidence showing how the vulnerabilities were prioritized, the actions taken or not taken, or methods used to verify the mitigations.

At Agency C, security issues found through penetration tests on applications were not resolved. Managers and staff said the agency did not prioritize remedying these vulnerabilities over other security issues due to constraints in resources and budgets. The agency could not provide any support for its processes or decisions because it lacked documentation. Documenting operational processes is important for quality and process control. Without proper documentation, it is difficult to monitor and evaluate if the operation was properly processed and completed.

Reasons for the gaps between OCIO standards and agency assessments varied

We asked staff and managers in agency IT divisions about the gaps we observed between our audit results and the expectations and requirements around assessments in Policy 141.10. In some instances, problems arose due to a misunderstanding of the full requirements, while other issues involved resources and agency priorities.

For example, staff at Agency A said they thought their current risk and vulnerability assessment processes complied with OCIO standards. They did not know that state policy required periodic risk and security assessments on applications specifically.

Staff at Agency B said their IT security team had been short-staffed for the past several years. The team only had one or two employees during this period, and they spent most of their time responding to security incidents, mitigating identified vulnerabilities, and maintaining IT security policies and procedures. Beginning April 1, 2023, the team was fully staffed to four employees, and could begin to address the areas that required its attention.

Staff at Agency C said they knew about the gap between state requirements and the agency's current risk and security assessment procedures. However, they said performing a formal assessment on applications was a complex and time-consuming process, and they lacked the resources necessary to meet state standards. Moreover, the agency's IT leadership did not recognize this as a priority. Staff perform ad hoc risk assessments when an application requires a significant change or update. Since Agency C lacks a formalized assessment process, this work – including findings and remediations – was not documented for us to review. The agency's goal is to formalize its risk and security assessment methodology to ensure it stays in compliance with state requirements.

Our review of agencies' own vulnerability scanning of servers identified potential security issues for their applications

Since all three agencies did not periodically perform state-required risk and security assessments on applications, we expanded our audit to see if we could identify vulnerabilities in their IT environment. We did this by reviewing data from the agencies' own vulnerability scans of servers housing their applications.

Our review identified multiple security vulnerabilities in applications that could cause a denial of application services, execution of arbitrary code, or disclosure of sensitive information. But because the agencies had not conducted proper IT application risk and security assessments, neither the audit team nor the agencies could determine how significantly those vulnerabilities could affect the applications or what other application vulnerabilities could be exploited.

Agencies could use qualitative and quantitative analysis to help them choose the best modernization option

Results in brief

Leading practices advise conducting both qualitative and quantitative analyses to identify options available to mitigate the risks associated with legacy applications. As part of the audit, we reviewed six IT modernization projects – two for each of the audited agencies – to see how each agency had arrived at its decisions. We found only one project where an agency had sufficiently analyzed all available options for modernization. Washington agencies could improve their decision-making process for choosing modernization options by conducting sufficient analyses and recording them.

Leading practices advise performing both qualitative and quantitative analyses to identify options available to mitigate the risks associated with legacy applications

Leading practices established for federal agencies advise them to consider the range of options available to mitigate the risks associated with their legacy applications. There are effectively four strategies to deal with the risks an organization has already identified:

- **Accept the risks and do not act.** Deciding to accept the risks associated with the legacy application and do nothing is still making an active choice.
- **Update the legacy system.** Update the application to improve its ability to handle the risks. This option does not provide new functionality but simply eliminates or reduces the risks associated with the existing functionality.
- **Enhance the legacy system.** In this option, the enhancements replace some elements of the application or add new functionality to address risks. The basic technology the application is built upon is retained.
- **Replace the legacy system.** Plan to retire and replace the legacy application with new, more advanced technology.

The final decision about which strategy to pursue should not be made without sufficient analysis. Typically, analyses should examine the risks, costs, and ultimate best value or return-on-investment that each choice offers.

According to the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource, federal agencies are responsible for establishing a decision-making process that addresses the life cycle of each information system, including end-of-service life. The process must include explicit criteria for analyzing the projected and actual costs, benefits and risks associated with the IT investments. At a minimum, agencies are expected to ensure that:

> ***"… decisions to improve, enhance, or modernize existing IT investments or to develop new IT investments are made only after conducting an alternatives analysis that includes both government-provided (internal, interagency, and intra-agency where applicable) and commercially available options, and the option representing the best value to the agencies has been selected."***

This federal guidance goes on to direct agencies to follow required documentation and document-retention steps, to demonstrate the analyses performed and how the agency arrived at its decision. The decision should be supported by materials explaining why the option selected was the best value for the agency.

In addition, the OMB Circular A-11, Capital Programming Guide, states that senior management might apply a benefit-cost or cost-effectiveness analysis at many key decision points in the capital programming process. Doing so can help executives decide whether the best way to reduce a performance gap is through acquiring a new capital asset, undertaking a major modification on an existing asset, or by some other method.

Washington agencies could improve their decision-making process for choosing modernization options by performing sufficient analyses and recording them

During the audit, we reviewed two IT application modernization projects at each agency for a total of six projects. We wanted to see whether and how each agency had arrived at its decisions, based on analyses it conducted. The results (listed below by agency) were mixed, with only one project, at Agency C, displaying a sufficient analysis of available options.

- **Agency A.** Documentation for both projects identified the risks of various modernization options, but did not include the risks of the selected option. In addition, agency staff said they reviewed different vendors' applications, but did not maintain the records supporting the results of that review. Due to the lack of records, we were unable to determine whether the agency analyzed vendor solutions.

- **Agency B.** Documentation for both projects showed the agency performed a high-level, risk-to-benefit analysis of options, but neither described which option was the best value to the agency.
- **Agency C.** For one project, the agency hired a contractor to perform multiple quantitative and qualitative analyses, including gap analysis, peer review, vendor analysis, a feasibility study, and cost-benefit analysis. The results helped the agency choose the best modernization option. This project had the most comprehensive analyses of all six we reviewed. However, in the case of the second project, Agency C did not maintain the records relating to its modernization option analysis, so we could not determine whether it considered other options or analyzed each option to make the best decision. When asked about the lack of documentation, agency staff said this was not a major IT project, and they were not sure who retained the original documentation.

We found all three agencies could improve their modernization decision-making process by performing additional analyses and recording them. Doing so would likely help managers prioritize the options available to them, aiding in selecting the best strategy for each legacy application. By retaining documentation, agencies meet the state requirement to keep records relating to the implementation of their applications/systems for six years. In addition, retaining documentation explaining their decisions would help them monitor and evaluate if the decision was properly made.

State Auditor's Conclusions

A thread throughout this performance audit is a simple idea – that Washington's state agencies should have a uniform and consistent approach to identifying legacy applications. Supporting that work with a statewide policy will be complex, but nonetheless important.

Legacy applications are more vulnerable to security threats, decreased performance and expensive maintenance. However, by their very nature, such applications vary as widely in their purpose and design as state agencies do in their core missions. Agencies may not have a definition of a legacy application. However, developing a definition will help them consistently identify applications whose age, risks and costs warrant the expense of replacement.

After reviewing the efforts of three state agencies, this audit makes several recommendations to develop a more uniform approach to identifying and tracking legacy applications, assess risks associated with those applications, and perform sufficient analyses of modernization options. In this effort, there is also a role for the state's Office of the Chief Information Officer to implement a statewide standard and policy for legacy applications.

Through these recommendations, state agencies can better track legacy applications, address the risks they present and plan for their ultimate replacement, which will help the state limit risk and deliver more effective service to Washingtonians in the long run.

Recommendations

For the audited agencies

To better identify and track legacy applications, as described on pages 12-19, we recommend the agencies:

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

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

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

For 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

Guidance for all 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. Therefore, we suggest all Washington state agencies consider the recommendations made to the audited agencies as they develop and implement their controls to manage legacy applications.

Agency Response

JAY INSLEE
Governor

WILLIAM S. KEHOE
Director &
State Chief Information Officer

STATE OF WASHINGTON
WASHINGTON TECHNOLOGY SOLUTIONS
Washington's Consolidated Technology Services Agency
1500 Jefferson Street SE ▪ Olympia, Washington 98504-1501

August 31, 2023

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

Dear Auditor McCarthy:

On behalf of the audited participants, thank you for the opportunity to review and respond to the State Auditor's Office (SAO) performance audit report "Controls to Manage Outdated Applications."

We agree on the importance of identifying and tracking legacy applications. The audited agencies will continue to update and review their IT application inventory data to ensure it is complete and accurate. We also agree that rigor around risk, vulnerability management, and security assessments is vital.

We appreciate that the report recognizes the potential risks and difficulties involved in utilizing legacy applications and the necessity of continuing to use these applications despite their inherent challenges.

We also welcome the report's insights and recommendations to improve legacy application management. WaTech is continually working to develop and improve the state's IT standards. However, reporting by agencies regarding compliance with the standards is inconsistent. Without full visibility into the status of legacy applications and platforms within state agencies, WaTech is limited in its ability assist with plans and support of funding requests for replacements or upgrades.

WaTech is fully committed to assisting organizations that rely on legacy software systems and platforms. WaTech can help agencies maintain the security of their legacy applications and platforms and ensure the confidentiality, integrity, and availability of all processed information. By identifying appropriate protective measures surrounding legacy applications and platforms, WaTech and agencies can extend the lifespan and improve the security of legacy systems and platforms, allowing sufficient time to properly plan for replacements and upgrades. The Washington State Legislature allocated $1.5 million in the FY 2023 budget to a legacy and modernization fund administered by WaTech to help accelerate legacy system modernization.

August 31, 2023
Washington State Auditor Pat McCarthy

Please thank your team for their professionalism throughout the audit process. We appreciate the information provided.

Sincerely,

William S. Kehoe
Director & State Chief Information Officer

cc: Jamila Thomas, Chief of Staff, Office of the Governor
Kelly Wicker, Deputy Chief of Staff, Office of the Governor
Rob Duff, Executive Director of Policy and Outreach, Office of the Governor
David Schumacher, Director, Office of Financial Management
Mandeep Kaundal, Director, Results Washington, Office of the Governor
Tammy Firkins, Performance Audit Liaison, Results Washington, Office of the Governor
Ralph Johnson, State Chief Information Security Officer, Washington Technology Solutions
Scott Frank, Director of Performance Audit, Office of the Washington State Auditor
Derek Puckett, Director of Policy & External Affairs, Washington Technology Solutions

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.

WaTech
Washington Technology Solutions

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

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.

WaTech
Washington Technology Solutions

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

- 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

WaTech
Washington Technology Solutions

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.

WaTech
Washington Technology Solutions

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

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."*

WaTech
Washington Technology Solutions

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

WaTech
Washington Technology Solutions

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

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.

State Auditor's Response

As part of the audit process, our Office provides a final draft of reports to audited entities and offers management an opportunity to respond. For this audit, these organizations also included Washington Technology Solutions (WaTech), and the Office of the Chief Information Officer (OCIO). Those responses are included in every published audit report. The state's response and action plan are included on pages 32-40 of this report. In this case, the response for two recommendations indicated that our recommendations had already been addressed by the agency. We summarize these items below, with our responses.

Implement a statewide standard and policy to identify and track legacy applications

In response to Recommendation No. 9, the OCIO concurred with the recommendation that it develop and implement a statewide standard and policy to identify and track legacy applications. The OCIO did not provide an action plan for this recommendation because it said the agency had already updated the current Technology Portfolio Foundations standards. However, this took place in June 2023 after we completed audit fieldwork.

Auditor's Response

We appreciate the OCIO's efforts to update the Technology Portfolio Foundations standards to add attributes to determine whether a given application is "legacy." However, the standard still lacks information about how state agencies should identify and track legacy applications. The standards do not specify what criteria or attributes agencies should use to determine whether an application qualifies as legacy. Therefore, we recommend the OCIO develop and implement a statewide standard and policy to identify and track legacy applications.

Implement a policy and process to ensure statewide application inventory records are complete and accurate

In response to Recommendation No. 10, the OCIO concurred with the recommendation that it 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. The OCIO did not provide an action plan for this recommendation because it said the agency currently examines the IT application inventory data and follows up with state agencies to discuss data accuracy when it is incomplete.

Auditor's Response

We appreciate the OCIO's efforts to ensure the statewide application inventory records are complete and accurate. However, our examination of statewide application inventory records showed they were not in fact complete and accurate. Therefore, we still recommend the OCIO implement the necessary policy or procedure to ensure the completeness and accuracy of statewide application inventory records.

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 sections of this report.

I-900 element	Addressed in the audit
1. Identify cost savings	**No.**
2. Identify services that can be reduced or eliminated	**No.**
3. Identify programs or services that can be transferred to the private sector	**No.**
4. Analyze gaps or overlaps in programs or services and provide recommendations to correct them	**No.**
5. Assess feasibility of pooling information technology systems within the department	**No.**

I-900 element	Addressed in the audit
6. Analyze departmental roles and functions, and provide recommendations to change or eliminate them	**No.**
7. Provide recommendations for statutory or regulatory changes that may be necessary for the department to properly carry out its functions	**No.**
8. Analyze departmental performance data, performance measures and self-assessment systems	**No.**
9. Identify relevant best practices	**Yes.** The audit used leading practices for identifying legacy IT systems, and prioritizing and executing legacy IT system updates or replacements.

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* (July 2018 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.

The mission of the Office of the Washington State Auditor

To provide citizens with independent and transparent examinations of how state and local governments use public funds, and develop strategies that make government more efficient and effective. The results of our work are widely distributed through a variety of reports, which are available on our website and through our free, electronic subscription service. We take our role as partners in accountability seriously. We provide training and technical assistance to governments and have an extensive quality assurance program. For more information about the State Auditor's Office, visit www.sao.wa.gov.

Appendix B: Objectives, Scope and Methodology

Objectives

The purpose of this performance audit was to answer the following questions for three selected state agencies:

1. Are there opportunities to improve their processes for identifying, tracking, 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?

Scope

This performance audit examined opportunities for selected agencies to improve their processes for identifying legacy applications and addressing risks associated with them. We selected three agencies based on factors like the number of old applications they have (see sidebar) and spending on the agency's operations. One selected agency's information technology (IT) administration is decentralized into multiple administrative units, each with its own IT division that autonomously manages unit IT operations. In this case, we selected one unit based on the same factors, such as the number of old applications and spending on the unit's operations.

This audit examined the selected agencies' processes for identifying legacy applications and addressing risks. It was not designed to identify which legacy applications should be modernized.

How the audit identified "old" applications

We considered an application to be old if it was older than 15 years. To identify the application's age, we used the application's service start date reported on the fiscal year 2020 statewide application inventory data that was maintained by Washington Technology Solutions (WaTech). As described on page 18 in the audit results, the service start date was missing for 2,539 applications, accounting for more than 40 percent of applications. Those applications were also considered to be old.

Methodology

We obtained the evidence used to support the findings, conclusions, and recommendations in this audit report during our fieldwork period (June 2022 to May 2023), with some additional follow-up work afterward. We have summarized the work we performed to address each of the audit objectives in the following sections.

Objective 1: Are there opportunities to improve selected agencies' processes for identifying and monitoring the use and maintenance of legacy applications?

To address this objective, we conducted a literature review to identify criteria and leading practices for defining and identifying legacy applications. This included reviewing guidance from the Office of Management and Budget (OMB) compliance requirements, standards and policies issued by Washington's Office of Chief Information Officer (OCIO), and other industry standards.

We also interviewed staff in the selected agencies' IT divisions to learn about their policies and procedures related to how they define and identify their legacy applications. None of the agencies had their own policies or procedure to define and identify legacy applications. Therefore, we evaluated agencies' current procedures for how they:

- Collect and update IT applications' key information
- Identify and monitor IT applications' maintenance cost
- Manage IT application defects and enhancement requests

Managing IT application inventory records

We requested and reviewed the selected agencies' policies and procedures, and interviewed staff in their IT divisions to learn about their current procedures for how they maintain IT applications' key information.

We obtained the agencies' 2021 and 2022 IT application portfolio inventory records to evaluate whether they were complete and accurate. We did not evaluate whether the inventory records cataloged all applications because we did not have a tool to identify all of them. Instead, we evaluated the completeness of the records by evaluating whether the agencies collected the minimum of 39 key application information fields that OCIO required to be reported. We selected applications based on how critical they are to the agencies' missions, and then examined the accuracy of the key information collected.

Identifying and monitoring IT applications' maintenance costs

We requested the selected agencies' policies and procedures, and interviewed staff in their IT divisions to learn about their current procedures for how they identify and monitor IT applications' maintenance costs.

We selected applications based on how critical they are to the agencies' missions, and requested and reviewed relevant documentation to assess if they identified, calculated, and monitored the maintenance cost for the selected applications accurately and completely.

Managing IT application defects and enhancement requests

We requested and reviewed the selected agencies' policies and procedures, and interviewed staff in their IT divisions to learn about their current procedure for how they manage IT application defects and enhancement requests.

We selected applications based on how critical they are to the agencies' missions. We obtained listings of defects and enhancement requests based on several factors, including the defect's criticality level and enhancement request's importance level. We requested and reviewed relevant documentation to assess if they were evaluated, prioritized and addressed.

We addressed the second and third objectives using similar techniques:

Objective 2: Do agencies assess risks for legacy applications to ensure they are appropriately secured, and support their business mission and objectives?

Objective 3: Do agencies have a strategy (or take corrective actions) to mitigate the risks identified for their legacy applications?

To address both objectives, we conducted a literature review to identify leading practices for application risk and security assessments, as well as guidance on how an organization can identify the best option to mitigate a legacy application's risks. This review included reviewing guidance from the OMB compliance requirements, OCIO standards and policies, and other industry standards.

We interviewed staff in the selected agencies' IT divisions to learn about their policies and procedures related to how they perform application risk and security assessments, and how they choose the best option with the highest effect and value.

We selected applications based on how critical they are to the agencies' missions. We requested and reviewed documentation relevant to risk and security assessments for the selected applications to assess if the agencies adequately performed risk and security assessments in accordance with state standards.

We also selected applications that agencies determined to modernize based on how critical the projects were to their agencies' missions. We requested and reviewed documentation relevant to the selected modernization projects to assess if the agencies sufficiently analyzed available options to choose the best one to address the risks associated with the existing applications.

Work on internal controls

Internal controls were significant to our audit objectives, which sought to identify opportunities to improve agencies' processes for identifying legacy applications and addressing risks associated with them. We reviewed controls that provide assurance:

- Agencies identify legacy applications consistently
- IT application inventory records are maintained accurately and completely
- IT application maintenance costs are calculated accurately and completely, and monitored
- IT application defects and enhancement requests are adequately evaluated, prioritized and addressed

- IT application risk and security assessments are performed in accordance with the state standard
- Agencies perform sufficient analysis to identify the best option to mitigate risks associated with legacy applications

Our audit looked to see if the three agencies implemented and followed these controls. We did not assess the operational effectiveness for these controls.

Reporting confidential or sensitive information

Because public distribution of tests performed and test results could increase the risk to the state, the public audit report does not present details of our work. We gave specific, detailed recommendations to the three agencies to improve their processes for identifying legacy applications and addressing risks associated with them.

Appendix C: Key Information Fields for Applications

This appendix lists 39 key information fields (attributes) for applications that OCIO required agencies to collect and report annually during the audit period. In June 2023, WaTech approved updates to application policy standard 112.10 including an updated Application and Infrastructure Inventory Template. The new template has 49 fields that agencies must track and submit to WaTech on an annual basis.

Field (Attribute)	Description of information required
Name	Name of the application
Description	Description of the item
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 organization's reputation *User Productivity* – If unavailable, there is impact to employee productivity
Business owner	Item owner or person responsible for this item
Technical owner	Technical or service owner responsible for this item
Life cycle status	Description of the item's life cycle: – In development or test – In production – Retirement in progress – Retired from inventory
Date acquired	Date the organization took ownership or entered software subscription
In service production date	Date application went into production. For applications that are capitalized, this date is associated with the date used for tracking useful life in agency asset tracking system. (See SAAM 30.20.70 – Depreciation Policy and SAAM 30.50.10.A Subsection 80 – Capital Asset Class Codes and Useful Life Schedule.)
Retirement date	Date removed from production

Field (Attribute)	Description of information required
Type of application	Description of the application type: – Custom/In-House – SaaS Software as a Service – PaaS Platform as a Service – COTS Commercial Off-the-Shelf – Hybrid Combination of application types
Manufacturer/ Vendor	Manufacturer/Vendor name
Cloud service provider	If applicable, name of the cloud service provider
Source supplier	Name of the seller of the item
Contract number	Reference to license or contract number
License number	Software license number
Version information	Software version number
Operating system	If applicable, list operating system name
Operating system version	If applicable, list operating system version
Key technologies	List programming language or platform used to develop application, such as C++, COBOL, JavaScript, .NET, Python, Salesforce, etc.
Authentication type	List authentication used to access the application, such as multifactor authentication, Active Directory, Secure Access Washington, etc.
Data security category	Does this application process, store, share, and/or transmit Category 3 or 4 data ? – Yes – No
Database relationship	If applicable, the infrastructure unique identifier associated with the database
Relationships to other infrastructure items	If applicable, list all other infrastructure unique identifiers associated with this application
Relationship to other applications	If this application is not a standalone application and is dependent upon another application for its existence, this application is considered a subsystem of another application. List the unique identifier of the primary application
Has resources available	If all required resources are available to run/support the application, the answer is Yes – Yes – No

Field (Attribute)	Description of information required
Is on an unsupported version	If the application is running on unsupported version of technology, the answer is Yes – Yes – No
Is updatable	If the application has all resources to update, the answer is Yes – Yes – No
Has other risks	If the agency has identified other risks associated with this application, the answer is Yes – Yes – No
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)
Integrates with federal or enterprise systems	If applicable, identify system the application integrates with: – Agency Financial Reporting System (AFRS) – Human Resource Management System (HRMS) – Travel and Expense Management System (TEMS) – Enterprise Contract Management System (ECMS) – Federal government system
Estimated user count	Number of end users accessing the application
Used by the agency	Identify if used by internal agency end users only – Yes – No
Used by the public	Identify if used by public end users providing or receiving data – Yes – No
Used by agency business partner	Identify if used by agency business partner end users who provide and receive data agency data – Yes – No
Used across government	Identify if used by governmental end users, such as city, county, state, tribal, education, etc. – Yes – No

Field (Attribute)	Description of information required
Location data	Identify if application relies on location-based data GIS data such as X,Y coordinates or mapping functionality – Yes – No
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. – Yes – No
Administrative or financial system	Identify if this application is an administrative or financial system. Link to Administrative and Financial System Definitions – Financial management – Management accounting – Budgeting – Travel management – Enterprise risk management – Grant/loan management – Procurement – Human resources

Field (Attribute)	Description of information required
Core business function	Identify the core business function the application supports – Administration – Analytical – Case management – Customer management – Data management – Development – Education/Training – Facilities – Financial – GIS – Health – Human resources – Informational – Law enforcement – Legal – Licensing – Project management – Safety – Scientific – Security – Other

Appendix D: OCIO Standard 141.10 Concerning Risk and Security Assessment

This appendix summarizes OCIO Standard 141.10 concerning risk and security assessment.

In February 2023, OCIO adopted new IT policies associated with the risk assessment that provide more structured, detailed guidance for the assessment process. **Figures 1** and **2** summarize OCIO standards used during the audit period. **Figures 3** and **4** summarize new OCIO standards in effect at the time of publication.

Figure 1 – Summary of OCIO Standard/Policy 141.10: Concerning ***risk*** assessments

Agencies must:
Define and implement a formal IT risk assessment process to evaluate risks resulting from the use of information systems to agency operations, systems and personnel.
Conduct an IT risk assessment when introducing new systems and making changes to an existing computing environment that impacts risk.
Conduct an IT risk assessment on systems processing Category 3 data or higher once every three years.
Conduct an IT risk assessment that contains the following assessment components: • Identify potential threats to assets • Identify the vulnerabilities that might be exploited by the threats • Identify the impacts that losses of confidentiality, integrity, and availability may have on assets • Assess the likelihood that security failures may occur based on prevailing threats and vulnerabilities • Take into account business, legal, or regulatory requirements, and contractual security obligations

Figure 2 – Summary of OCIO Standard/Policy 141.10: Concerning ***security*** assessments

Agencies must:
Establish an IT security assessment framework and schedule to identify a sampling of agency systems, applications, and IT infrastructure to test. Examples of periodic testing include penetration tests and vulnerability assessments.
Conduct IT security assessments against the sample in the framework to verify security controls and identify weaknesses at least once every three years.
Conduct an assessment through testing scenarios relevant to changes made when the following conditions exist: a. A significant IT infrastructure upgrade or modification since the last IT security assessment was performed b. Applications have been added or significantly modified
Correct weaknesses identified with appropriate controls.

Figure 3 – Summary of new OCIO 141.10: Concerning *risk management*, adopted February 11, 2023

Agencies must:
Define and document a risk strategy appropriate to their mission.
Identify the security categorization of its systems based on the data processed.
Authorize and document their risk management strategy (as it applies to procurement of a new information system or if there are significant changes to an existing information system's technology or in the data categories it stores, processes or transmits. This is accomplished by agencies submitting a Risk Treatment Plan (RTP) for review per the Security Assessment and Authorization Policy.
Implement their system and environment monitoring strategies. This includes an annual update to the system risk assessment

Figure 4 – Summary of new OCIO Standard/Policy 141.10: Concerning *risk assessment*, adopted February 11, 2023

Agencies must:
Conduct risk assessments at critical points: • Prior to acquisition of an information system, cloud service or managed service which processes CAT 3 or 4 data • When an existing agency-controlled information system undergoes a significant change in technology • At least once every three years for all agency-controlled information systems that process CAT 3 or CAT 4 data • Annually for information systems the agency deems to be business essential • Prior to the sharing of CAT 3 or CAT 4 data with agencies or vendors • When a security patch is not applied
Prepare for the risk assessment by identifying the purpose, scope, assumptions and constraints, threat intelligence sources, and risk model and analytic approach.
Conduct risk assessments to identify threat sources, threat events, likelihood, impact and risk
Communicate and share risk assessment results to appropriate agency decision makers and interested parties to support risk response.

"Our vision is to increase **trust** in government. We are the public's window into how tax money is spent."

– Pat McCarthy, State Auditor

Washington State Auditor's Office
P.O. Box 40031 Olympia WA 98504

www.sao.wa.gov

1-564-999-0950

Office of the Washington State Auditor
Pat McCarthy