PERFORMANCE AUDIT

Report Highlights

Office of the Washington State Auditor
Pat McCarthy

Controls to Manage Outdated IT Applications

Washington's governments use information technology (IT) applications every day to perform many critical functions, from providing social services to collecting taxes. 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 These products use outdated technology, are often incompatible with more modern IT systems, and are challenging to maintain. In fact, Washington Technology Solutions (WaTech), 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 when they are incompatible with modern security features. The applications 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 legacy applications, keeping accurate and complete application inventory records, and monitoring maintenance costs

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. Once identified, agencies should maintain accurate and complete IT application inventories to 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 inventories limit management's ability to make informed decisions, and they affect the accuracy of statewide inventory records.

Report number 1033149, published 9/5/2023, online at www.sao.wa.gov

We also 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

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

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.

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. These 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. 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. 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

We made a series of recommendations to the three audited state agencies to better identify legacy applications and address risks associated with them. We also noted guidance for all state agencies to consider our report's findings as they manage legacy applications of their own.