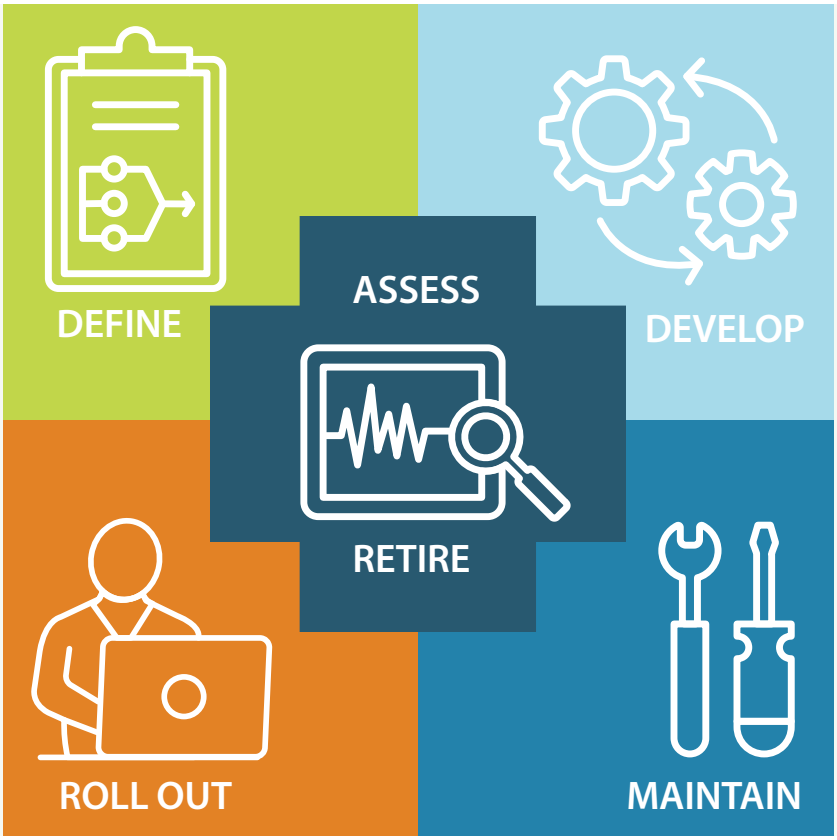
Center for Government Innovation

Office of the Washington State Auditor
Pat McCarthy

Managing Outdated IT Applications

Leading practices to help local governments address "legacy systems"



Washington governments, large and small, use IT applications every day to perform many critical functions, from supporting public safety and providing social services to collecting taxes and managing public transportation. 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.

A recent performance audit looked at three state agencies to see how they managed applications that might be nearing the end of their useful life.

Read the full performance audit, **Controls to Manage Outdated Applications**, on our website at sao.wa.gov/reports-data/audit-reports/controls-manage-outdated-computer-applications

September 2023

IT applications have a natural lifespan. Here are tips to know when to retire them!

Each application has a lifespan, illustrated in the five steps at right. An essential aspect of maintaining applications – step 4 – includes preparing for step 5. You and your IT department or service provider should be able to identify the point at which any has reached retirement age and should be given its gold watch.

Those used beyond the point where they might be retired are frequently called "legacy applications." Washington Technology Solutions (WaTech), the state's centralized provider and procurer of IT services, estimates that between 40 percent and 60 percent of state agencies' applications should be considered legacy.

Local governments that use outdated applications face many of the same risks as state agencies:

- More vulnerable to cyberattacks when they are incompatible with modern security features and can no longer be updated adequately
- Slow, inefficient processing of data, and more likely to fail outright, which can affect a government's ability to achieve its objectives
- Out of compliance with evolving state or federal regulations and standards
- Expensive long-term costs of maintaining legacy systems can outweigh the trouble and expense of transitioning to new software

How do I know if this software is out-of-date?

A useful starting point is the definition of a legacy application proposed by the state's Office of the Chief Information Officer (OCIO) at WaTech.

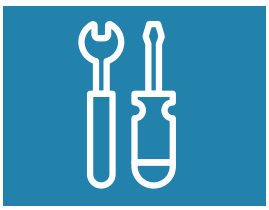
- The system cannot be easily updated due to complicated or unclear code, fragile interfaces, or lack of documentation.
- Maintenance or modification of the system depends on expertise that is hard to find or prohibitively expensive.
- The system depends on software no longer supported by the vendor.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

IT application life cycle stages

1. Define application requirements

2. Develop or buy the application

3. Roll out application to users



4. Maintain and improve as needed

5. Assess and plan for eventual retirement

How do I identify the problem?

The performance audit found that the audited agencies lacked policies or guidelines that established criteria for a legacy application. For your local government to effectively manage the risks legacy applications pose to security, efficiency and costs, you must first recognize which software 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.

Until you know what applications you have, however, it's very difficult to develop your maintenance and replacement plans. A great next step is to develop and maintain a catalog of all those your government uses.

Ensure the catalog entries capture the data you need to make informed decisions, including basic information about the application. The OCIO requires state agencies to report data in 43 different inventory fields. The audit identified 23 key fields that can underpin a useful application inventory for most governments – they're listed in the box below.

Nine inventory fields in particular can be used to identify a legacy application, including service start date (indicating an application's age), operating system and key technologies. They're marked with a symbol like this: ♦

Recommended fields for an application inventory

Description	License number	Relationships to other applications
Technical owners	Version information	♦ In-service date
Business owners	♦ Operating system	Business criticality
Date acquired	♦ Operating system version	♦ Is updatable
Manufacturer/Vendor	♦ Authentication type	♦ Has resources available
Cloud service provider	♦ Key technologies	♦ Is running on an unsupported version
Source supplier	Database relationship	♦ Has other risks
Contract number	Relationships to other infrastructure	

Mitigating the problems you find

If all this inventorying and monitoring seems like a lot of extra work for your already overstretched IT team, consider this: The more you're aware of potential problems, the better your ability to make sound decisions. The audit explained that incomplete and inaccurate information on IT application maintenance costs also limited 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 or 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. But at the end of the day, you have four basic strategies to pursue. The more information you have about your information technology, the better placed you are to choose a wise course of action.

An organization effectively has four strategies available to deal with the risks it identifies in outdated systems. Don't select one until you've given the problem sufficient analyses, examining the risks, costs, and ultimate best value or return-on-investment that each choice offers.

- **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.