

# Outdated applications and conversions

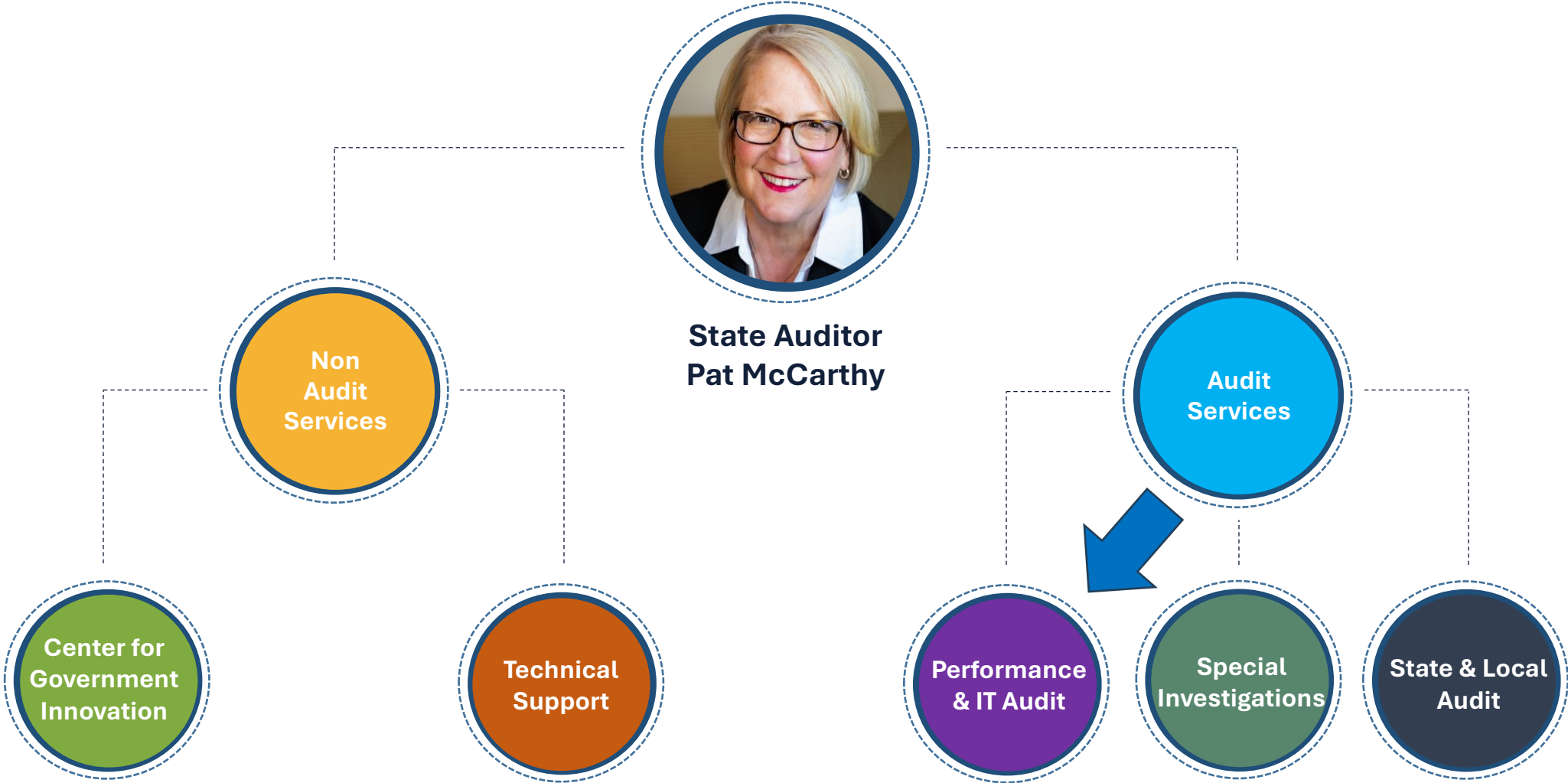
Be aware of outdated system risks and be prepared for conversions

Sonya Singh | IT System Assistant Audit Manager  
Audrie Shellhart | IT Systems Auditor



Office of the Washington State Auditor

# About SAO





# Agenda

## **Outdated Applications:**

- Business critical applications
- Risks with outdated applications
- What to do about these risks

## **Conversions:**

- Selecting a new application
- Moving data
- User access impacts
- Interfacing impacts
- Data backup recovery impacts
- Patch management impacts



The background of the slide features a collage of business-related imagery. On the left, there is a calendar showing months like May, June, July, and October. In the center, a clock face is visible with hands pointing to approximately 10:10. On the right, a bar chart with several vertical bars of varying heights is shown. The entire background is in a light blue and white color scheme.

# What are business essential and mission critical applications?



The background of the slide features a collage of three elements: a calendar showing months like May, June, July, and October; a clock face with hands pointing to approximately 10:10; and a bar chart with several vertical bars of varying heights. The entire background is in a light blue, semi-transparent style.

# What is an outdated applications?

- Outdated technology
- No longer supported
- Lack of personnel



# Sharing data



SHARING DATA FROM ONE  
DEPARTMENT TO ANOTHER



SHARING DATA TO OTHER  
AGENCIES



The background features a collage of time-related imagery. On the left, a calendar shows months from May to November. In the center, a clock face is visible with hands pointing to approximately 10:10. On the right, a bar chart with three bars of increasing height is shown. The overall color scheme is light blue and white.

# What are risks related to outdated application?





# Risks with outdated application

Increased  
vulnerability to  
security threats



Disruption in  
functionality



Decreased  
productivity



Not meet  
standards and  
compliance





# Common Identified Issues

Not having  
procedures

Not  
performing risk  
assessments

Not mitigating  
and addressing  
risks



# What do you do?



IDENTIFY AND EVALUATE  
APPLICATIONS



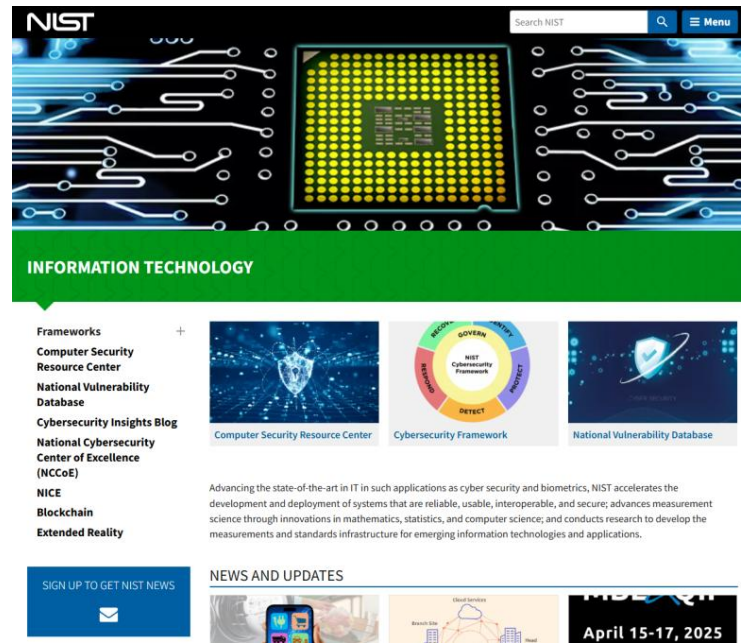
CONDUCT RISK  
ASSESSMENTS



MITIGATE THE RISKS



# SAO Resources





# Conversions



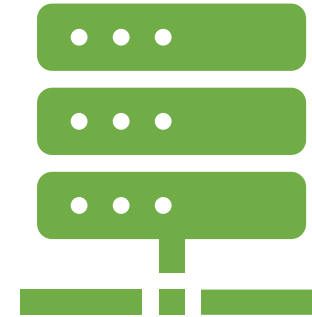


# What's a conversion?





Data moving from one spot to another



Version changes, platform changes,  
server changes, whole system changes





# Selection

- Business needs
- Bidding and compliance requirements
- Similar systems





STAFF PROPERLY  
TRAINED



NEW CONTROLS



HAVING A PLAN



CREATING A  
FLOWCHART OF DATA



Office of the Washington State Auditor



# Data



Office of the Washington State Auditor



TRANSACTION  
HISTORY



RATE TABLES



ACCRUAL RATES



OUTSTANDING  
BALANCES



Office of the Washington State Auditor



**CLEAN UP DATA**



**KNOW WHERE  
HISTORICAL DATA**



**RETAIN TESTING  
DOCUMENTATION**



Office of the Washington State Auditor



# Common issues

Not retaining testing  
reconciliations/validations



Not having a plan



Not ensuring data is  
complete and accurate



# Software Conversion Resource





# Did you backup?

- Perform backup before and after the conversion
- Re-evaluate existing procedure



# Common issues

Lack	Lack of procedures, plans and documentation
Lack	Lack of vendor monitoring
Lack	Lack of test restores



# Backup Recovery Resource



The background of the slide features a collage of time-related imagery. On the left, there is a calendar showing months like May, June, July, and October. In the center, a clock face is visible with hands pointing to approximately 10:10. On the right, a bar chart with several vertical bars of varying heights is shown. The overall color scheme is light blue and white.

# How are you going to Patch the new system?

- Who's responsible for patching? IT or Vendor?



## Common issues



LACK OF PROCEDURES



LACK OF MONITORING

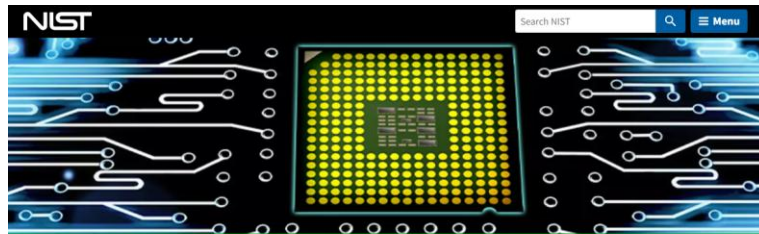


LACK OF EVALUATION



Office of the Washington State Auditor

# Patch Management Resources



**INFORMATION TECHNOLOGY**

**Frameworks**

- Computer Security Resource Center
- National Vulnerability Database
- Cybersecurity Insights Blog
- National Cybersecurity Center of Excellence (NCCoE)
- NICE
- Blockchain
- Extended Reality

Advancing the state-of-the-art in IT in such applications as cyber security and biometrics, NIST accelerates the development and deployment of systems that are reliable, usable, interoperable, and secure; advances measurement science through innovations in mathematics, statistics, and computer science; and conducts research to develop the measurements and standards infrastructure for emerging information technologies and applications.

**NEWS AND UPDATES**

April 15-17, 2025



**The 18 CIS Critical Security Controls**

The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices that you can use to strengthen your cybersecurity posture.

This latest version, CIS Controls v8.1, includes updated alignment to evolving industry standards and frameworks, revised asset classes and Safeguard descriptions, as well as the addition of the "Governance" security function.

Click on the individual CIS Control for more information:

- CIS Control 1: Inventory and Control of Enterprise Assets
- CIS Control 2: Inventory and Control of Software Assets
- CIS Control 3: Data Protection
- CIS Control 4: Secure Configuration of Enterprise Assets and Software
- CIS Control 5: Account Management
- CIS Control 6: Access Control Management
- CIS Control 7: Continuous Vulnerability Management

**CIS Controls™**

**CIS CONTROLS V8.1 AND RESOURCES**

**LEARN ABOUT IMPLEMENTATION GROUPS**

**CIS Controls™ Community**

**JOIN A COMMUNITY**

Looking for Previous Versions?

**ACCESS V8 RESOURCES AND TOOLS**

**ACCESS V7.1 RESOURCES AND TOOLS**



The background of the slide features a collage of three elements: a calendar showing months like May, June, July, and October; a clock face with hands pointing to approximately 10:10; and a bar chart with several vertical bars of varying heights. The text is overlaid on this collage.

# Does the system interface to any other applications?





# User Access



Office of the Washington State Auditor



PROTECT DATA



MINIMIZE RISK OF  
UNAUTHORIZED ACTIVITIES



Office of the Washington State Auditor

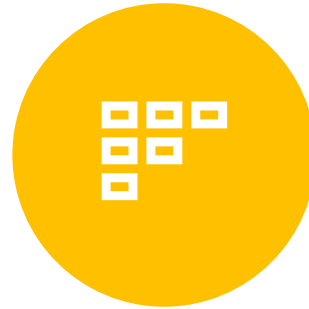
## Common issues:



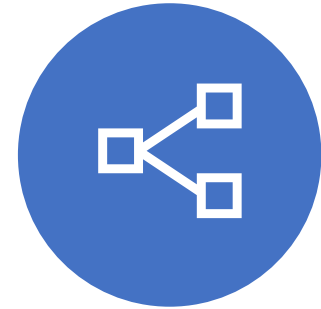
LACK OF POLICIES



LACK OF  
MONITORING



LACK OF LIMITED  
ACCESS



LACK OF SEPARATION  
OF DUTIES



Office of the Washington State Auditor



# Vendor Management



Monitor activities



Monitor transactions



Monitor data



Office of the Washington State Auditor



# Vendor Management

Help with  
trouble  
shooting

Help with  
data transfer

Help with  
service  
accounts



Office of the Washington State Auditor

# Common issues



NO WRITTEN  
CONTRACTS



LACK OF MONITORING



LACK OF EVIDENCE






## Improve your cybersecurity without breaking your budget

**Center for Government Innovation**  
Office of the Washington State Auditor  
Pat McCarthy

Balancing the many needs and budget priorities of your local government is challenging and finding dollars for cybersecurity programs may seem monumental. Would you be surprised to learn there are tools you can use at little to no cost? Here, we have rounded up some of the best resources available to help you improve your cybersecurity posture.

- 1. Multi-State Information Sharing and Analysis Center (MS-ISAC) offers free membership with many benefits.**  
As a local government, this is your key resource for cyber threat prevention, protection, response and recovery! MS-ISAC is funded by the Department of Homeland Security, so it has many free and low cost services, such as immediate help should you experience a cyber incident. MS-ISAC's operations center is available 24/7, and offers free incident response services like emergency conference calls, mitigation recommendations and forensic analysis.
- 2. Cybersecurity & Infrastructure Security Agency (CISA), a division of Homeland Security, offers services at no cost.**  
CISA, a division of Homeland Security, offers free services to local governments including vulnerability scanning, phishing campaign assessment, and remote penetration testing. For a complete list of services, see <https://www.cisa.gov/cyberresources>.
- 3. The Public Infrastructure Security Cyber Education System (PISCES) helps small local governments.**  
PISCES connects small municipalities (fewer than 150 network users) with students who analyze live-streaming metadata, and perform network and threat analyses. CISA and Pacific Northwest National Laboratory support PISCES, and it started here in Washington.

March 2022



## Segregation of Duties

### Essential Internal Controls

Why it matters:  
How to get started:  
Helpful tools for local governments:  
Pros, self-assessments and checklists

Published by the Center for Government Innovation  
Office of the Washington State Auditor  
Pat McCarthy, September 2021



## CYBERSECURITY

is everyone's job.

**It starts with policy**

A guide to jump-starting your cybersecurity program

The Office of the Washington State Auditor launched the Cyber Checklist program in 2021, and one of the common results we have found is that local governments lack or need to improve their information technology (IT) documentation, including standards, procedures and most importantly, policies.

Here are what different groups need from your IT policies to **#BeCyberSmart**.

**Leadership and Planning**

Office of the Washington State Auditor  
Pat McCarthy  
September 2024

# Resources



# Summary:

## **Outdated Applications:**

- Identify and evaluate

## **Conversions:**

- Evaluate the application
- data is complete and accurate
- application interfaces
- Perform Backups before and after the conversion
- Ensure patches are monitored
- Perform user access reviews six months after going live and there after according to internal policies



# Questions?



Office of the Washington State Auditor

# Information

**Audrie Shellhart**

**IT Systems Auditor**

**[Audrie.Shellhart@sao.wa.gov](mailto:Audrie.Shellhart@sao.wa.gov)**

**(564) 201- 2964**

**Sonya Singh, MS-ITAM**

**IT Systems Assistant Audit Manager**

**[Sonya.Singh@sao.wa.gov](mailto:Sonya.Singh@sao.wa.gov)**

**(360) 594-0614**

**Karen Wilson, CPA, CISA**

**IT Systems Program Manager**

**[Karen.Wilson@sao.wa.gov](mailto:Karen.Wilson@sao.wa.gov)**

**(509) 581-3990**

Website: [sao.wa.gov](http://sao.wa.gov)

Twitter: [@WaStateAuditor](https://twitter.com/WaStateAuditor)

Facebook: [facebook.com/WaStateAuditorsOffice](https://facebook.com/WaStateAuditorsOffice)

