

How resilient is your cybersecurity program?

How SAO is helping government prepare for cyber threats

Dan Mann, CISSP

Center for Government Innovation Cybersecurity Specialist

Deena Garza

Port and IDC Program Manager

Washington Public Ports Association

October 26, 2023



Office of the Washington State Auditor

Today's agenda

01 What's going on in local audit

02 Resources at your fingertips

03 Cyber checkups

- Purpose
- Process
- Other audits

04 Q&A



RCW 43.09.185

Updated in 2022:

“State agencies and local governments shall immediately report to the state auditor's office known or suspected loss of public funds or assets or other illegal activity. ***The state auditor must adopt policies as necessary to implement this section.***”

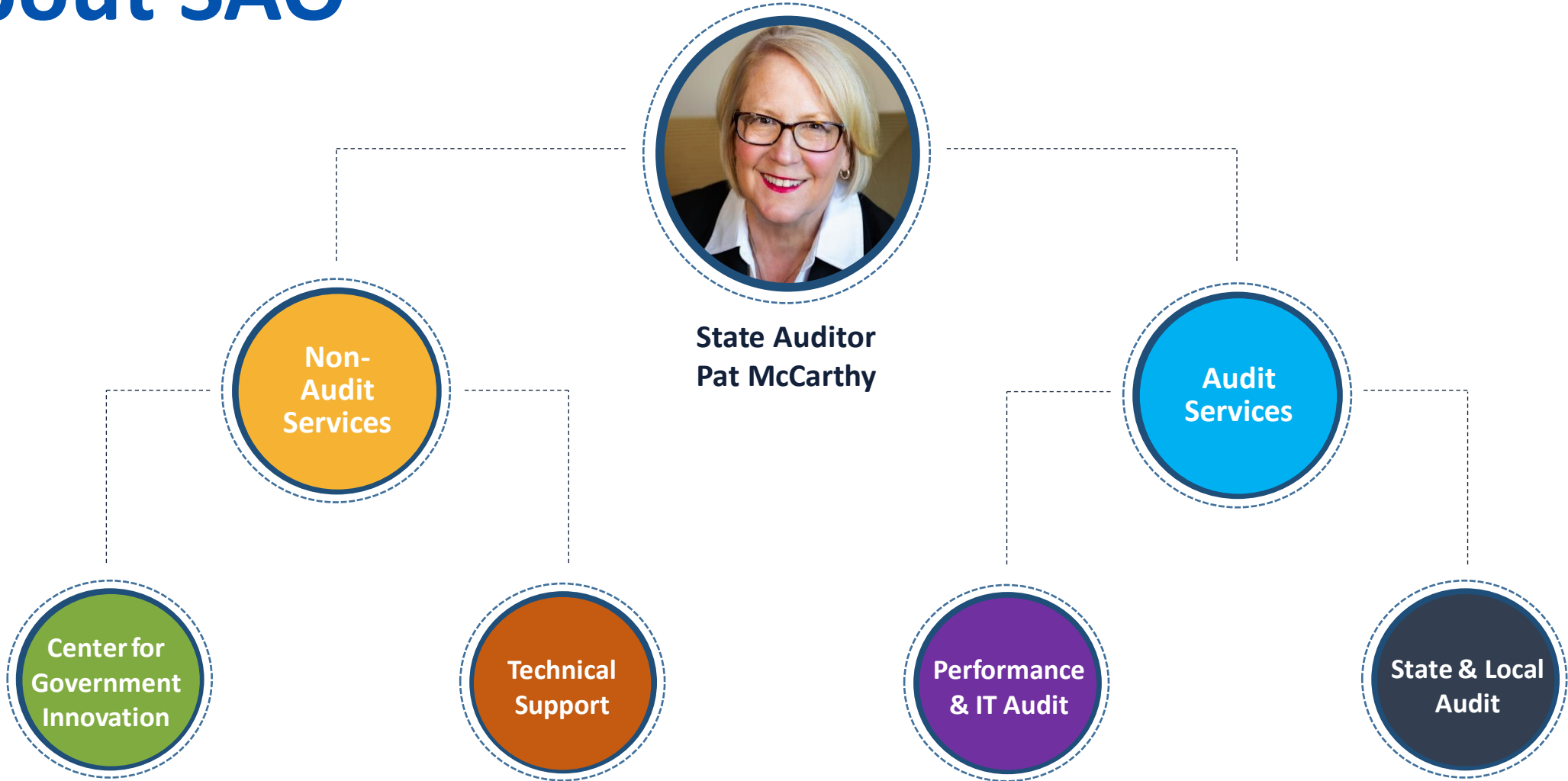


Scan QR code to read the [updated policy](#) on our website!

SAO's new loss reporting policy



About SAO





General Loss Reporting Policy (effective August 17, 2023)

SAO is in the process of adding additional sections to this policy, which will clarify fraud reporting requirements for specific government entities and agencies. We will publish new sections of the policy on this page as they are finalized.

[Expand all](#)

Overview +

Section 1: Losses or Illegal Activities Exempt from Reporting Requirement +

Section 2: Clarification of Losses to Report Cybersecurity Incidents +

For questions about fraud procedures or the fraud program, contact us at fraud@sao.wa.gov.



Do not need to report:

- Unauthorized credit card attempts and/or transactions initiated by an external party, that are determined fraudulent by the bank and refunded.
- Loss of cellphones, tablets, laptops or similar type assets assigned to employees that were stolen by an external party.



Reporting exceptions



If in doubt,
report it!

If employee involvement cannot be ruled out in any of the listed exemptions, governments should report the loss or illegal activity to SAO.

“Employee involvement” means the scheme involved or was carried out by an employee of the affected government.



Reminder! Do report:

Cybersecurity incidents that involve the finances or financial records in some way.

- Payment to a criminal actor (even if your insurance paid it or reimbursed you).
- Ransomware or other unauthorized access where it's possible they accessed any financial records (even if no harm or no ransom paid).



Reporting cyber losses



The Center's resource library can help you manage your port's day-to-day business

Accounts payable & receivable

Cash receipting

Payroll

Assets

Cybersecurity

Federal funds



Fraud prevention

Procurement

Public records & OPMA

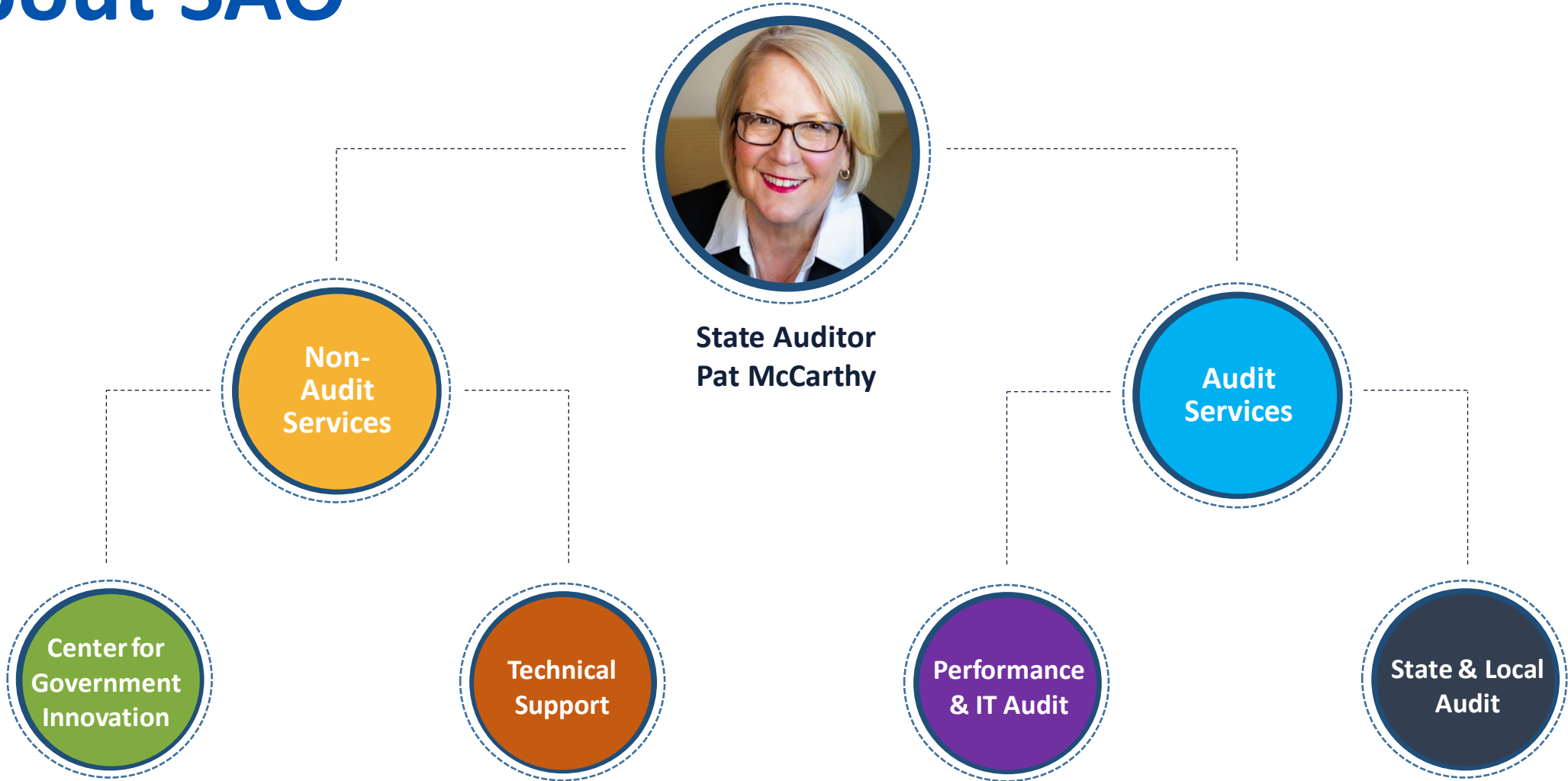
GAAP & cash-basis financial reporting

Revenues & expenditures

Technology



About SAO



Online Resource Library



The screenshot shows the website for the Office of the Washington State Auditor's Resource Library. At the top, there is a navigation bar with links for 'The Audit Connection Blog', 'Coronavirus', 'Public Records', 'Client Login', and social media icons for Facebook, Twitter, LinkedIn, and YouTube. The main header includes the state seal, the text 'Office of the Washington State Auditor Pat McCarthy', and a search bar labeled 'Search SAO'. Below this is a secondary navigation bar with categories: 'Reports & Data', 'Performance Audits', 'About Audits', 'Improving Government', 'BARS & Annual Filing', 'Report a Concern', and 'About SAO'. The breadcrumb trail reads 'SAO HOME / IMPROVING GOVERNMENT / Resource Library'. The main content area is titled 'Resource Library' and contains a left sidebar with a menu of resources: 'The Center for Government Innovation', 'Lean Services', 'Teambuilding Workshops', '#BeCyberSmart', 'Financial Intelligence Tool', 'Resource Library' (highlighted), 'Technical Advice', '#Gov101', 'Improvement Training Videos', and 'Presenting Fraud'. The main content area features a paragraph stating that the SAO provides free guides, checklists, best practices, and tools to help Washington governments improve internal controls, grants management, procurement practices, financial reporting, and cybersecurity. It then lists categories for browsing: 'Internal Controls' (with buttons for ACCOUNTS PAYABLE, CASH RECEIPTING, PAYROLL, and ASSETS), 'Compliance' (with buttons for PROCUREMENT and FEDERAL FUNDS), 'Financial Reporting' (with buttons for GAAP BASIS and CASH BASIS), 'Government Operations' (with buttons for OPERATIONS, LEAN SERVICES, REVENUES, and EXPENDITURES), and 'Organizational Safeguards' (with buttons for CYBERSECURITY, TECHNOLOGY, and FRAUD PREVENTION). A 'Featured resource' section highlights a guide titled 'Trust, but verify: A guide for elected officials & appointed boards to prevent fraud', with a 'View/download PDF' link. Below this, there is a question 'Want to know when SAO releases new resources?' and another featured resource titled 'In the KNOW with SAO'.



Helpful checklists

- Resource is regularly updated
- Customizable
- Logical categories
- Useful for more than just the preparer
- Gives insight into future best practices



The image shows a checklist titled "Checklist for Preparing Cash Basis Financial Statements" from the Center for Government Innovation. The checklist includes a header with the Washington State Auditor's Office logo and the Center for Government Innovation logo. Below the header, there are fields for "Date of Review:", "Completed by:", and "Key recommendations:". The main body of the checklist consists of a table with columns for "Question", "Yes", "No", "N/A", and "Comments". The questions are numbered 1 through 7 and cover various aspects of financial statement preparation, such as journal entries, subsidiary ledgers, reconciliations, and BARS changes. A footer at the bottom right indicates "Page 1 of 2".

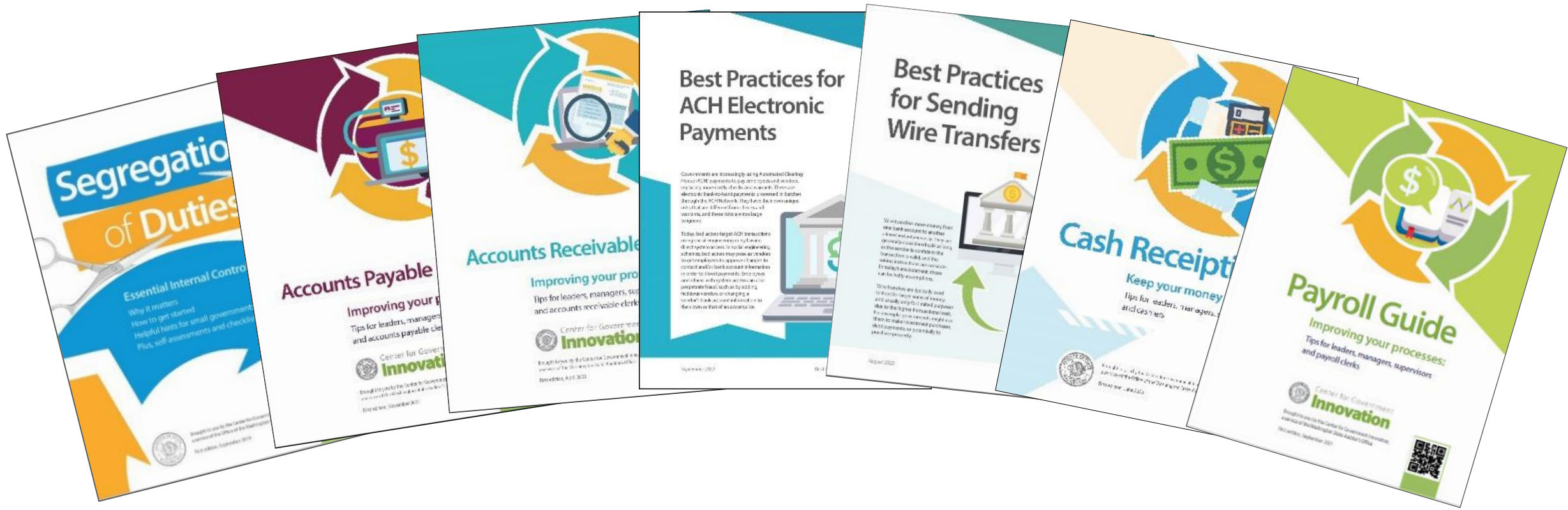
Question	Yes	No	N/A	Comments
1. Are all journal entries completed, supported and reviewed by someone other than the preparer?				
2. Are the subsidiary ledgers reconciled to the general ledger (the ledger on which the financial statements are based) regularly? <i>Note: Subsidiary ledger information generates source information included in the general ledger, such as a utility billing system; reconciliations can identify discrepancies or printing errors that might reflect inaccurate information.</i>				
3. Have the general ledger cash and investment balances been reconciled each month with hard-copy documents (such as bank statements or county treasurer reports) (BARS 3.1.9.5)?				
4. Have the general ledger revenues been reconciled to total cash receipts, as shown by banking or county treasurer records? <i>Note: Maintaining a list of reconciling amounts between cash receipts and revenues will help in performing a proof of cash, providing amounts for Schedule 06 and detecting irregularities.</i>				
5. Have the general ledger expenditures been reconciled to total cash payments, as shown by banking or County Treasurer records? <i>Note: Maintaining a list of reconciling amounts between cash payments and expenditures will help in performing a proof of cash, providing amounts for Schedule 06 and detecting irregularities.</i>				
6. Does the general ledger reflect all of the local government's activity? <i>Note: For example, if the court has a separate bank account, then the cash and related activity should be included in the general ledger and the financial statements.</i>				
7. Does someone other than the preparer of the reconciliations monitor to ensure they have been completed accurately and in a timely manner?				



Earn CPE
with our
free, on-
demand
training



Looking to improve your internal controls? The Center can help!



Cyber resources & training from the Center

#BeCyberSmart



Cyber resources by role

CYBERSECURITY
is everyone's job.

Leading the way
Cybersecurity considerations for local government leadership

Local government leadership sets the tone for cybersecurity in their communities. Local government leaders have a unique opportunity to lead by example and ensure that their communities are secure and resilient. Here are three things you can do in your role to #BeCyberSmart.



Office of the Washington State Auditor
Pat McCarthy

CYBERSECURITY
is everyone's job.

Protecting facilities
Increasing use of software and connectivity presents risks

As the use of software and connectivity increases in local government, the risk of cyberattacks also increases. Local government leaders have a unique opportunity to lead by example and ensure that their communities are secure and resilient. Here are three things you can do in your role to #BeCyberSmart.




Office of the Washington State Auditor
Pat McCarthy

CYBERSECURITY
is everyone's job.

Understanding laws and risks
Legal implications drive compliance and mitigation efforts

Local government leaders have a unique opportunity to lead by example and ensure that their communities are secure and resilient. Here are three things you can do in your role to #BeCyberSmart.



Office of the Washington State Auditor
Pat McCarthy

CYBERSECURITY
is everyone's job.

Finance matters
Considerations extend beyond budget decisions

As a finance or administrative professional in a local government, you have key responsibilities for managing that government's resources. In your role, you interact with all aspects of a local government's operations as you inform budgetary decisions. Here are three things you can do in your role to #BeCyberSmart.



Office of the Washington State Auditor
Pat McCarthy

CYBERSECURITY
is everyone's job.

At the core of cybersecurity
IT staff can help build, integrate and maintain a cybersecurity program

Local government IT staff are the backbone of a local government's cybersecurity program. They are responsible for building, integrating and maintaining a cybersecurity program that protects the community's data and systems. Here are three things you can do in your role to #BeCyberSmart.




Office of the Washington State Auditor
Pat McCarthy

CYBERSECURITY
is everyone's job.

People matter in cybersecurity
Local government human resources involvement is essential

Human resources professionals have a unique opportunity to lead by example and ensure that their communities are secure and resilient. Here are three things you can do in your role to #BeCyberSmart.



Office of the Washington State Auditor
Pat McCarthy



Other cyber resources

Center for Government Innovation



Office of the Washington State Auditor
Pat McCarthy

Improve your cybersecurity without breaking your budget

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/cyber-resource-hub>.


- 3. The Public Infrastructure Security Cyber Education System (PISCES) helps small local governments**

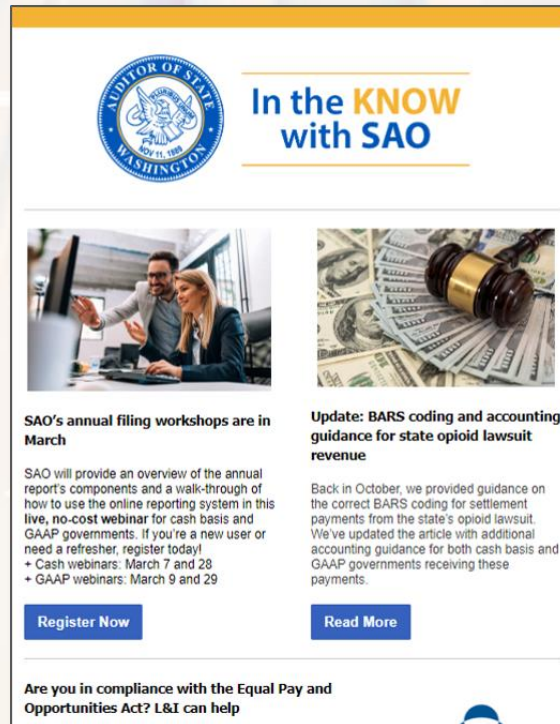
PISCES connects small municipalities (fewer than 150 network users) with students who analyze live-streaming metadata, and perform network and threat analyses. CISA and Pacific Northwest National Laboratory support *PISCES*, and it started here in Washington.



 March 2022



Subscribe to SAO's e-newsletter



Two ways to sign up:

1. Via SAO's website at sao.wa.gov
2. Use the QR code below:



Types of cyber work at SAO

		Engagement Type			
		Cyber Checkup	Critical Infrastructure Audit	Ransomware Resiliency Audit	CIS Safeguards Audit
Types of Work	Controls Assessment	Interviews, documentation, & limited evidence	Limited to one interview w/o evidence	Interviews, documentation, evidence, & technical testing	Interviews, documentation, evidence, & technical testing
	External Penetration Testing	No	Unauthenticated only	No	Comprehensive, depending on scope
	Internal Penetration Testing	No	No	No	Comprehensive, depending on scope
	In-house technical Testing	Limited	No	Comprehensive, depending on scope	Comprehensive, depending on scope



Program goal

To help local governments understand and build their own cybersecurity programs to minimize their risk of attack, data breach and/or financial loss

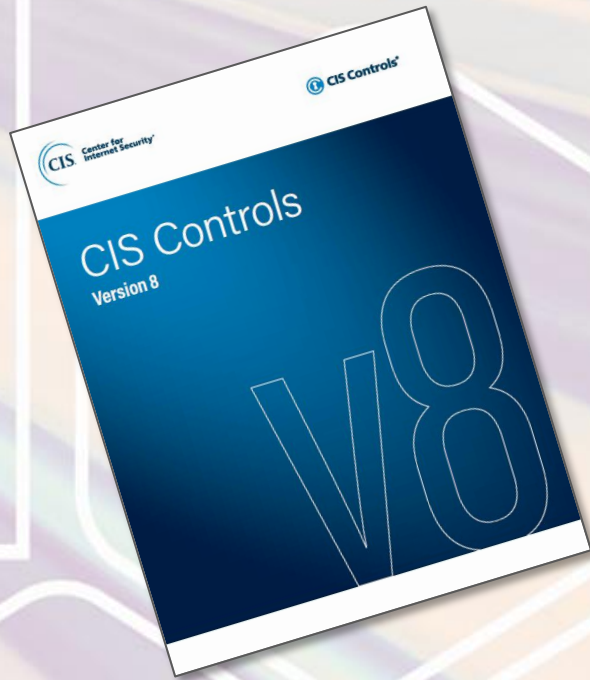
Target audience

- Smaller local governments
- Those that have experienced a confirmed or suspected cybersecurity breach
- Those who are on SAO's IT Audit waiting list and match the other selection criteria



Cyber Checkups





Cyber Checkups

What is a cyber checkup?

A free, 20-point inspection that diagnoses cybersecurity gaps that could leave a government vulnerable to common threats and offers recommendations on how to address them.

What are they based on?

- The framework provided by the Center for Internet Security's (CIS) Critical Security Controls, Version 8.0.
- SAO's cybersecurity audits are based on the same control framework.



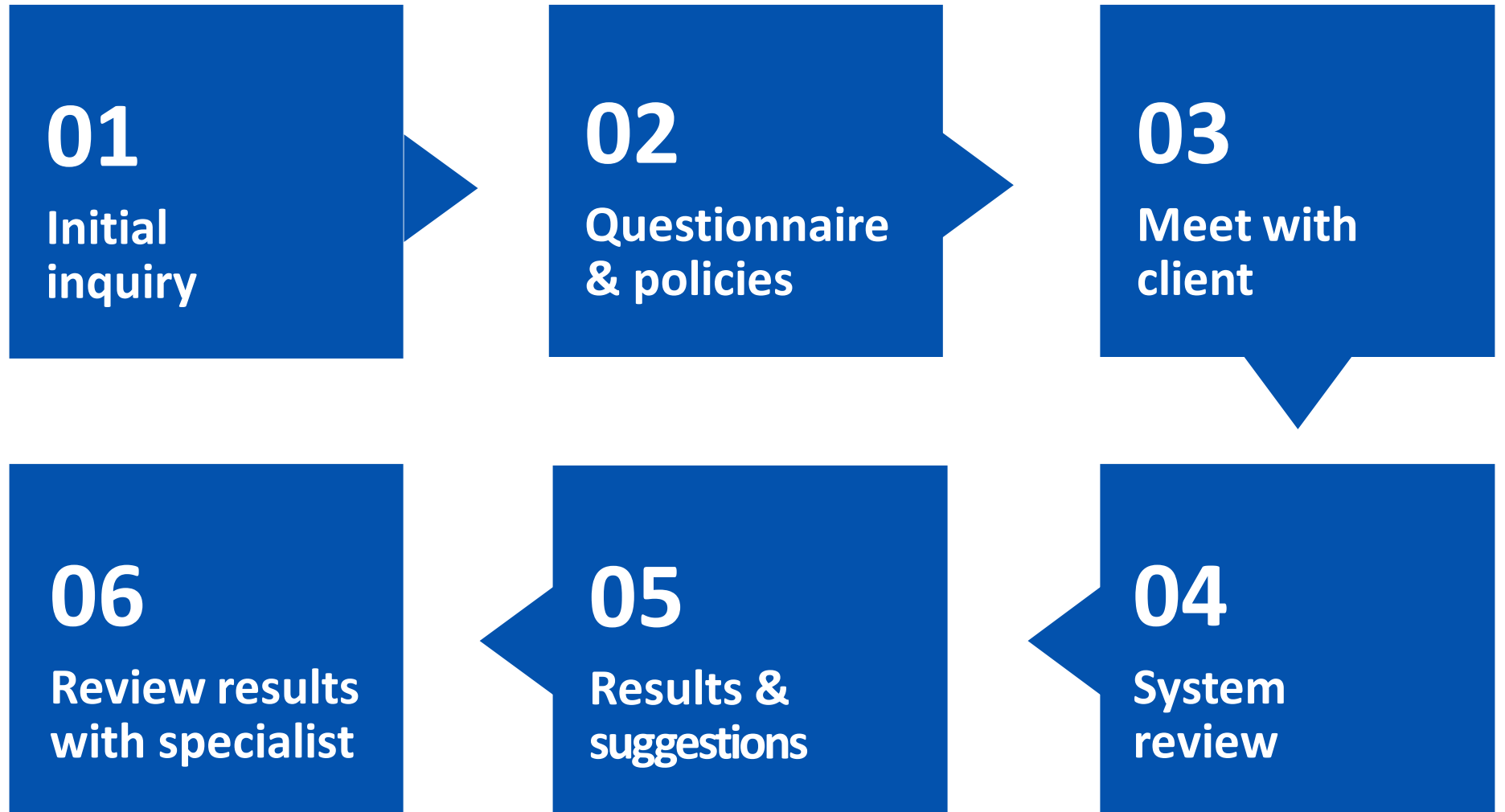
Control selection guidelines

- No external software needed for testing, and it's noninvasive
- No elevated privileges required for the testing
- No IT experience needed to answer questions
- Tests could be done quickly
- Were in CIS Controls implementation group 1

Cyber Checkups



Cyber checkup process



Questionnaire

The image shows a screenshot of a questionnaire titled "Cyber Checkup Questionnaire" from the Center for Government Innovation and the Office of the Washington State Auditor. The form includes a header with logos, an introductory paragraph, and three numbered questions with multiple-choice options. Question 1 asks about IT support, Question 2 asks about written IT policies and employee notification, and Question 3 asks about cybersecurity awareness training. The form also includes a footer with a disclaimer and the hashtag #BeCyberSmart.

Center for Government Innovation
Office of the Washington State Auditor

Cyber Checkup Questionnaire

We look forward to working with you to improve your government's cyber defenses. As part of our cyber checkup, we ask that you fill out the following questionnaire to the best of your ability. If you have IT support (internal or external), we encourage you to work with them to answer the questions below. If you don't know an answer, it's okay to leave the question blank.

Name of organization: _____
Number of employees: _____

1. Who provides your organization's IT support?
 We have our own IT staff of _____ (fill in # of IT employees)
 We have our own IT staff and also contract with a third-party service provider
 We use our county's IT staff
 Other: _____
 We don't have support from IT staff or a third-party provider
 I'm not sure

2. Does your organization have written IT policies?
 Yes, we have a written IT policies
 No, we don't have written policies
 I'm not sure

If you answered 'yes' to the question above, how are employees notified about IT policies?
(Check all that apply)
 During the onboarding process after new employees are hired
 During periodic employee training
 When policies are updated
 Other: _____
 I'm not sure

3. Do employees receive cybersecurity awareness/prevention training?
 Yes, all employees receive training
 Yes, but only certain employees receive training
 No, we don't provide training
 I'm not sure

If you answered 'yes' to the question above, how frequently do your employees receive cybersecurity training? (Check all that apply)
 During the onboarding process after new employees are hired
 Annually
 When policies are updated
 Other: _____

Limited distribution - Confidential and proprietary SAO information, subject to RCW 42.56.420 and RCW 42.56.270.

#BeCyberSmart

20 questions with multiple choice answers or short responses

Questions address specific questions

Typical user can answer



Additional info

IT policies

Incident response plan

Systems settings review

City of Mayberry	No: 2017-003
Information Technology	Updated: June 2022
IT Standard	Issued By: Mayor
Remote Access	Owner: City Administrator

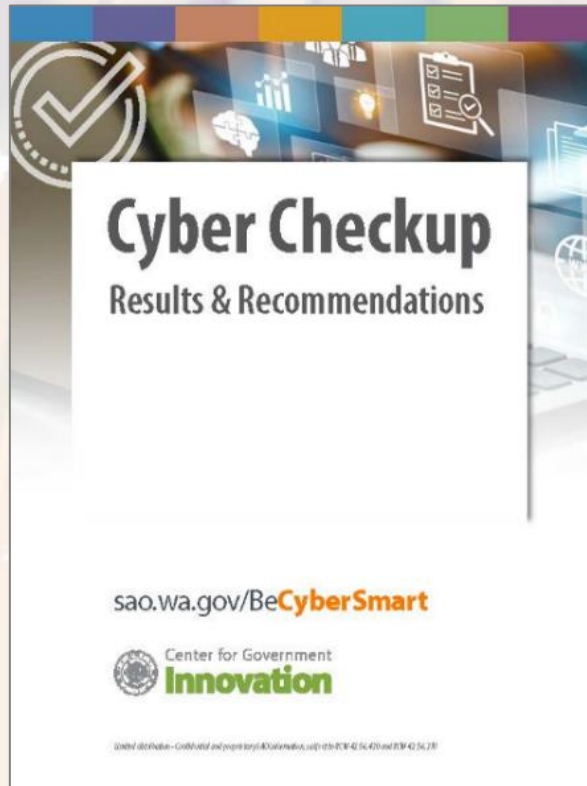
1.0 Purpose and Benefits

The purpose of this standard is to establish authorized methods for remotely accessing resources and services securely.

Major security concerns with remote access include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external hosts, potential damage to resources, and unauthorized access to information.



Summary



Summary document

Executive summary

Introduce other Center services



Overview

Grouped together

Dashboard on a single page

Color-coordinated by area


Cyber Checkup Results: Overview

Area	#	Does your organization...?	Strength of your safeguard		
			Strong	Needs improvement	Not implemented
Policies & Training	1.	Establish and maintain written IT policies	✓		
	2.	Have a cybersecurity awareness program in place		✓	
Incident Response	3.	Have a process for employees to report cybersecurity incidents		✓	
	4.	Designate a lead and a backup to oversee incident response and recovery			✓
	5.	Maintain an inventory of emergency contacts and service providers			✓
Accounts & Passwords	6.	Require employees to use strong and unique passwords	✓		
	7.	Encourage employees to use password managers	✓		
	8.	Restrict administrator privileges to dedicated administrator accounts	✓		
	9.	Protect accounts with administrative privileges by using multifactor authentication (MFA)	✓		
	10.	Require remote workers to use MFA		✓	
Computers & Other Devices	11.	Install anti-virus programs on all computers	✓		
	12.	Regularly apply security patches on all computers and applications			✓
	13.	Use only fully supported browsers and email clients			✓
	14.	Apply timed lockouts on all device screens	✓		
Data Protection	15.	Encrypt data on computers or other devices containing sensitive information	✓		
	16.	Back up data regularly and automatically		✓	
	17.	Block unnecessary email attachments		✓	
Network	18.	Maintain firewalls on all computers and devices	✓		
	19.	Use DNS filtering services to block access to malicious domains	✓		
Credit Cards	20.	Meet PCI DSS requirements for credit cards	✓		

Cyber Checkup Results & Recommendations | 3



Safeguards

Accounts & Passwords 

Safeguard 9: Protect accounts with administrative privileges by using multifactor authentication (MFA)

About this safeguard

This safeguard addresses a common technique for protecting accounts with administrative privileges: multifactor authentication (MFA). Multifactor means users can only access certain computer systems or applications if they possess two of these security elements: 1) Something they know, such as a password, pin, or answer to a security question; 2) Something they have, such as a cell phone where they can retrieve a texted code, a hardware security key, or a smart card with an embedded chip; or 3) Something they are, usually a biometric like a fingerprint or voice recognition.

Why this safeguard is important

Accounts with administrative privileges should be protected with MFA because of the increased risk to the IT system if they are compromised. MFA adds an extra layer of authentication that hackers are unlikely to be able to replicate when trying to log into your government's computer system.

For example, MFA using a smartphone will send a unique verification code to the administrator's device after the employee has entered their user name and password. The correct code must be entered into the system before the application will unlock. Even with a stolen user name and password, hackers are unlikely to have access to the smartphone connected to the user account. Without the verification code, hackers will have more difficult time trying to access the system.

What we observed during the checkup

Our recommendations

- Check with your IT support or service provider whether MFA is being used on accounts with administrative privileges. If not, determine what is needed to implement MFA on these accounts.
- If software your government uses came with a MFA option, make sure it is enabled for all accounts with administrative privileges. If you're unsure if MFA is available, contact your software vendor to find out the steps you need to take to activate it.
- If MFA isn't an option with your current software or service, evaluate whether you want to keep using that product or service, or find something new with better security features.
- Be sure your IT policy includes requirements for MFA on administrative accounts.
- If your government can't implement MFA right now, refer to Safeguard 8 for suggestions on improving security for administrative accounts.

Resources and references you can use

- Cybersecurity & Infrastructure Security Agency (CISA) offers a succinct summary of [multifactor authentication](#).
- Microsoft provides an overview of the [types of administrative accounts](#) that should have MFA enabled as well as sample policy language.

This safeguard supports [CIS Controls 6.5](#)

Cyber Checkup Results & Recommendations | 14

Detailed description

Consistent layout

Observations during checkup

Recommendations



Questions?



Contact information

Daniel Mann

Cybersecurity Specialist

Center for Government Innovation

Center@sao.wa.gov

(564) 999-0818

Deena Garza

Port and IDC Program Manager

Deena.Garza@sao.wa.gov

(360) 594-0571

Website: www.sao.wa.gov

X (formerly known as Twitter): @WAStateAuditor

Facebook: www.facebook.com/WaStateAuditorsOffice

LinkedIn: Washington State Auditor's Office



Cybersecurity Awareness



Sign up for quick-assessment “cyber checkups” offered by the Center

Introducing audits to address attacks that result in government “cyber losses,” including ransomware attacks

Adding 18 additional governments to our critical infrastructure audit project

Conducting more full cybersecurity audits of local governments

