In the KNOW with SAO

Deena Garza
Port Program Manager

Scott Woelfle
Director Quality Assurance and Innovation

Joanna Bailey
Lean Specialist Center for Government Innovation

Washington Public Ports Association
June 25, 2025

Agenda

01	02	03	04
Preparing for an audit	Fraud prevention	Resources from the Center for Government Innovation	Lean for ports

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:

About SAO

State Auditor
Pat McCarthy

- Non-audit services
  - Center for Government Innovation
  - Technical support
- Audit services
  - Performance & IT audit
  - State & local audit

Audits and findings, by the numbers

Every year, we issue thousands of reports, reflecting the results of many different kinds of audits. Just a small percentage of the audits find a significant problem – in other words, a "finding." Here's what we did on the public's behalf in fiscal year 2024:

2,724 audits

July 1, 2023 – June 30, 2024

1,127 audits

136 findings

Accountability audits

Accountability audits determine whether public funds are accounted for and if controls are in place to protect public resources from loss, misappropriation and abuse.

777 audits

86 findings

Financial audits

Financial audits determine whether the financial statements present an accurate picture of a government's finances.

477 audits

260 findings

Federal audits

Federal audits determine whether federal money is being used according to federal regulations.

Preparing for audit

- Open a line of communication before the audit start date
- Make good use of a “pre-audit” meeting with the audit team – who should attend

- Keep your files current and complete
- Learn from the past. Review your government’s past audit results

- Assess changes in activities
- Remember to document, document, document throughout the year

Preparing for audit

- Document your internal processes and recording financial transactions properly
- Be aware of changing accounting standards

- Perform a self-review of the annual report
- Develop an audit timeline and assign responsibilities

Relax! You've done all you can and are now ready for audit.

Audit timeliness takes a team effort

- SAO's priority is to work with you on timely and cost-effective audits
- Be sure to identify and communicate your audit needs
  - Bond deadlines
  - Federal grant compliance deadlines (Single Audit)
- Make good use of pre-audit meetings
- Regular audit status meetings keep us both on track
- Work with your auditors to have a plan in place for providing audit documents

What are audits going to look at?

- Accountability
- Financial Statements
- Federal grant compliance

What auditors might emphasize in upcoming accountability audits

- **Electronic fund transfers (EFTs)**
- **Payroll leave** (accruals, tracking and buyouts)

Financial statement reporting

Risks to consider:

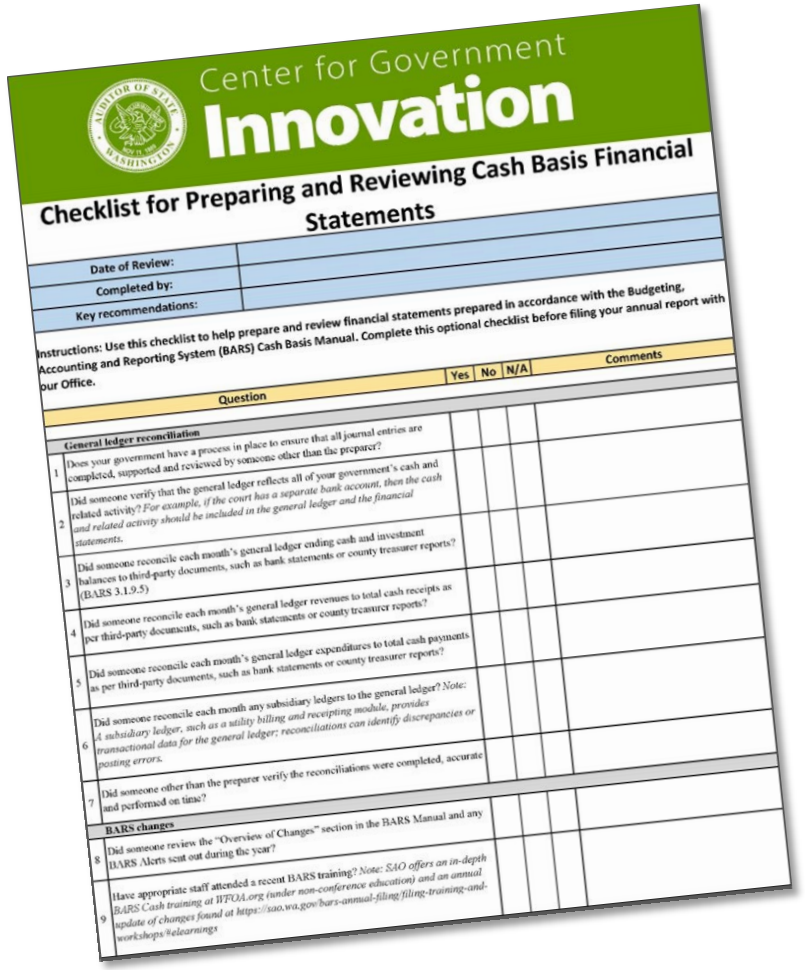
- Inadequate review of the prepared financial statements
- Lack of documentation evidencing review performed
- Outdated note disclosures, missing information and numerical errors

Helpful tips:

✓Always use the most up-to-date version of the BARS Manual

✓Consider using the “Checklist for Preparing Cash-Basis Financial Statements” for preparation and review

Resource: financial statement reporting checklist



Center for Government Innovation

Checklist for Preparing and Reviewing Cash Basis Financial Statements

Date of Review:	
Completed by:	
Key recommendations:	

Instructions: Use this checklist to help prepare and review financial statements prepared in accordance with the Budgeting, Accounting and Reporting System (BARS) Cash Basis Manual. Complete this optional checklist before filing your annual report with our Office.

	Question	Yes	No	N/A	Comments
	General ledger reconciliation				
1	Does your government have a process in place to ensure that all journal entries are completed, supported and reviewed by someone other than the preparer?				
2	Did someone verify that the general ledger reflects all of your government's cash and related activity? *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.*				
3	Did someone reconcile each month's general ledger ending cash and investment balances to third-party documents, such as bank statements or county treasurer reports? (BARS 3.1.9.5)				
4	Did someone reconcile each month's general ledger revenues to total cash receipts as per third-party documents, such as bank statements or county treasurer reports?				
5	Did someone reconcile each month's general ledger expenditures to total cash payments as per third-party documents, such as bank statements or county treasurer reports?				
6	Did someone reconcile each month any subsidiary ledgers to the general ledger? *Note: A subsidiary ledger, such as a utility billing and receipting module, provides transactional data for the general ledger; reconciliations can identify discrepancies or posting errors.*				
7	Did someone other than the preparer verify the reconciliations were completed, accurate and performed on time?				
	BARS changes				
8	Did someone review the "Overview of Changes" section in the BARS Manual and any BARS Alerts sent out during the year?				
9	Have appropriate staff attended a recent BARS training? *Note: SAO offers an in-depth BARS Cash training at WFOA.org (under non-conference education) and an annual update of changes found at https://sao.wa.gov/bars-annual-filing/filing-training-and-workshops/#elearnings*				

- Updated annually to include new BARS requirements and other accounting changes
- Covers several aspects of the financial statements, including funds structures, cash and investments balances, required schedules, and more

Find this and other financial reporting tools in our online Resource Library

Common recommendations in federal compliance audits

- Suspension and Debarment *
- Reporting requirements
- Procurement requirements *
- Davis-Bacon/Certified Payrolls *

* Also a top recommendation area for port districts

Federal awards compliance

Section 2 Chapter 8

Suspension and debarment

Before you enter into a covered transaction, the Uniform Guidance requires you to verify whether a contractor or subrecipient is suspended, debarred or otherwise excluded from receiving or participating in federal awards. This requirement is easy to comply with, but it is a common issue for local governments because it can be overlooked during the procurement process or when issuing subawards. While rare, paying federal funds to a suspended or debarred party could lead your auditor to question costs which may result in you having to repay the money to the awarding agency.

This chapter defines covered transactions and identifies the three ways of verifying suspension and debarment status. The chapter concludes with an overview of the procedures that local governments can expect their auditors to perform, as well as links to additional resources.

An overview of requirements

You must verify the suspension and debarment status of third parties before entering into a "covered transaction" with them. For most local government recipients, covered transactions typically include the following (exceptions are rare):

- Contracts for goods and services awarded, including professional service contracts, that are expected to equal or exceed $25,000 in accordance with 2 CFR §180.220(b)(1).

  Note: This applies to each contract, as well as total purchases from one contractor during the fiscal year for like-kind items. It also applies to contracts funded in whole, or in part, with federal funds.

- All subawards given to subrecipients (including other governments), irrespective of award amount, unless they are exempt under 2 CFR §180.215.

  Note: You must consider each new subaward a new transaction, which requires you to reverify suspension and debarment status.

Three ways of verifying suspension and debarment status

Before you enter into a covered transaction, you must verify that the person (or entity) with whom you intend to do business is not excluded or disqualified. The Uniform Guidance (2 CFR §180.300) identifies three ways you can do this:

- Obtain a signed certification from the third party attesting they are not suspended or debarred
- Insert a clause into the contract stating the third party is not suspended or debarred

Section 2 Chapter 10

Reporting

Almost every federal award requires recipients to file reports, which could include financial, performance and other special reporting. For example, a request for reimbursement is a type of financial report that governments commonly submit. However, governments often struggle with some of the reporting requirements tied to their federal awards. They may report inaccurate information or even fail to file their reports at all. Awarding agencies rely on reports to ensure recipients used award funds to achieve program objectives. Since awarding agencies use this information to make future funding decisions, it is important for recipients to fulfill all their reporting requirements and submit accurate information.

This chapter explains how to find your reporting responsibilities and summarizes the certification requirements and subaward reporting obligations. The chapter concludes with an overview of the procedures that local governments can expect their auditors to perform, as well as links to additional resources.

An overview of requirements

The federal agency or awarding agency should describe the reporting requirements in your award's terms and conditions. The Uniform Guidance includes reporting requirements, but much of it focuses on what federal agencies may require of recipients. You can find this guidance at 2 CFR §200.328 and 2 CFR §200.329.

Federal agencies or pass-through agencies may require reporting on an accrual basis, but they cannot require a recipient or subrecipient to establish an accrual accounting system. If you maintain your records on some other basis, you may develop accrual data for your reports based on an analysis of the documentation on hand, as per 2 CFR §200.302(b)(2).

Certifying reports

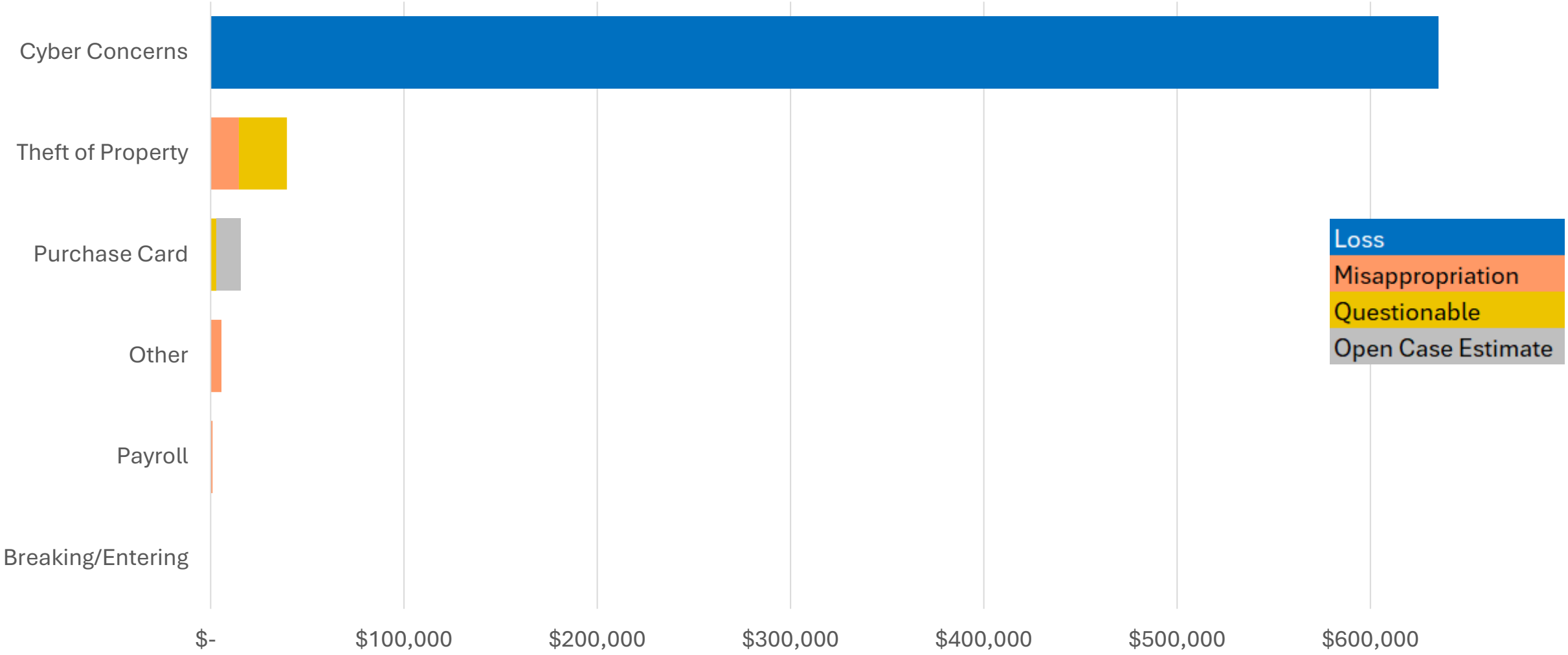
The Uniform Guidance (2 CFR §200.415) requires recipients to certify their financial reports. An official who is authorized to legally bind the recipient must sign the certification with language that comes directly from the Uniform Guidance, which says:

> "By signing this report, I certify to the best of my knowledge and belief that the report is true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, Section 1001 and Title 31, Sections 3729-3730 and 3801-3812)."

Fraud Prevention

Sometimes the best prevention is just being informed

Most costly fraud schemes



Fraud warning signs

4. Email address is not an exact match, or is an outside address when it should be internal

5. Request comes via email when you have a different method setup, or comes to the wrong department

6. Request comes in close to payment date and/or creates a sense of urgency

Inconsistent email addresses

Real	Spoofed
@g-o.com	[name].g-o.com@hotmail.com
@spfr.org	@spsfr.org
@bosscontruction.biz	@bossconstructions.biz
@AmericanGuardServices.com	@AmericanGuradServices.com
Vendor: Nisqually Construction	@NisquallyContracting.com
@mpmediatv.com	@messagepolntmedia.com

Emails from “employees”

Emails sent from
myprivatesecurebox01@gmail.com
myprivateboxinfo1@gmail.com
calorygas@telefonica.net
Info.ce0executives@lycos.com
schools@unifieddistrict.net
Theboysandgirlsclubs@sapo.pt
nies71@sznlive.com

Fraud warning signs

3. Provides a voided check that anyone could create, and/or a typed signature

4. Email address is not an exact match, or is an outside address when it should be internal

5. Request comes via email when you have a different method setup, or comes to the wrong department

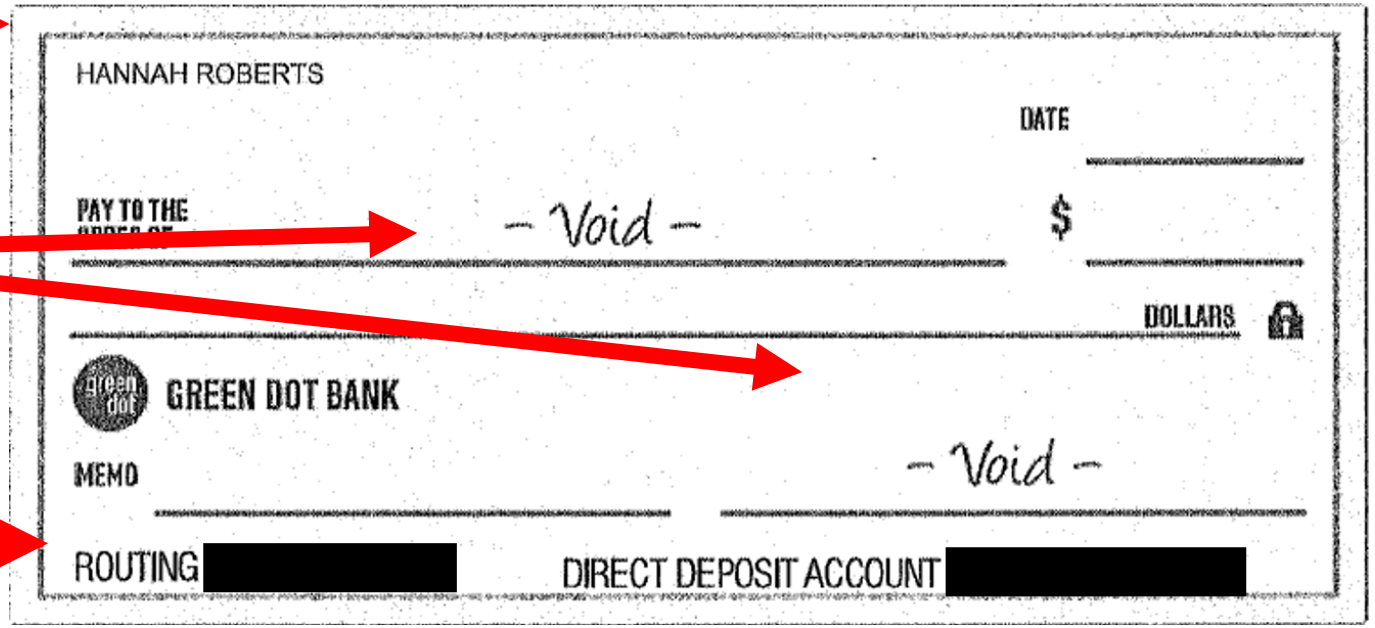
6. Request comes in close to payment date and/or creates a sense of urgency

Phony voided check

No address block

Likely typed with a script font

Atypical listing of routing and account information



Fraud warning signs

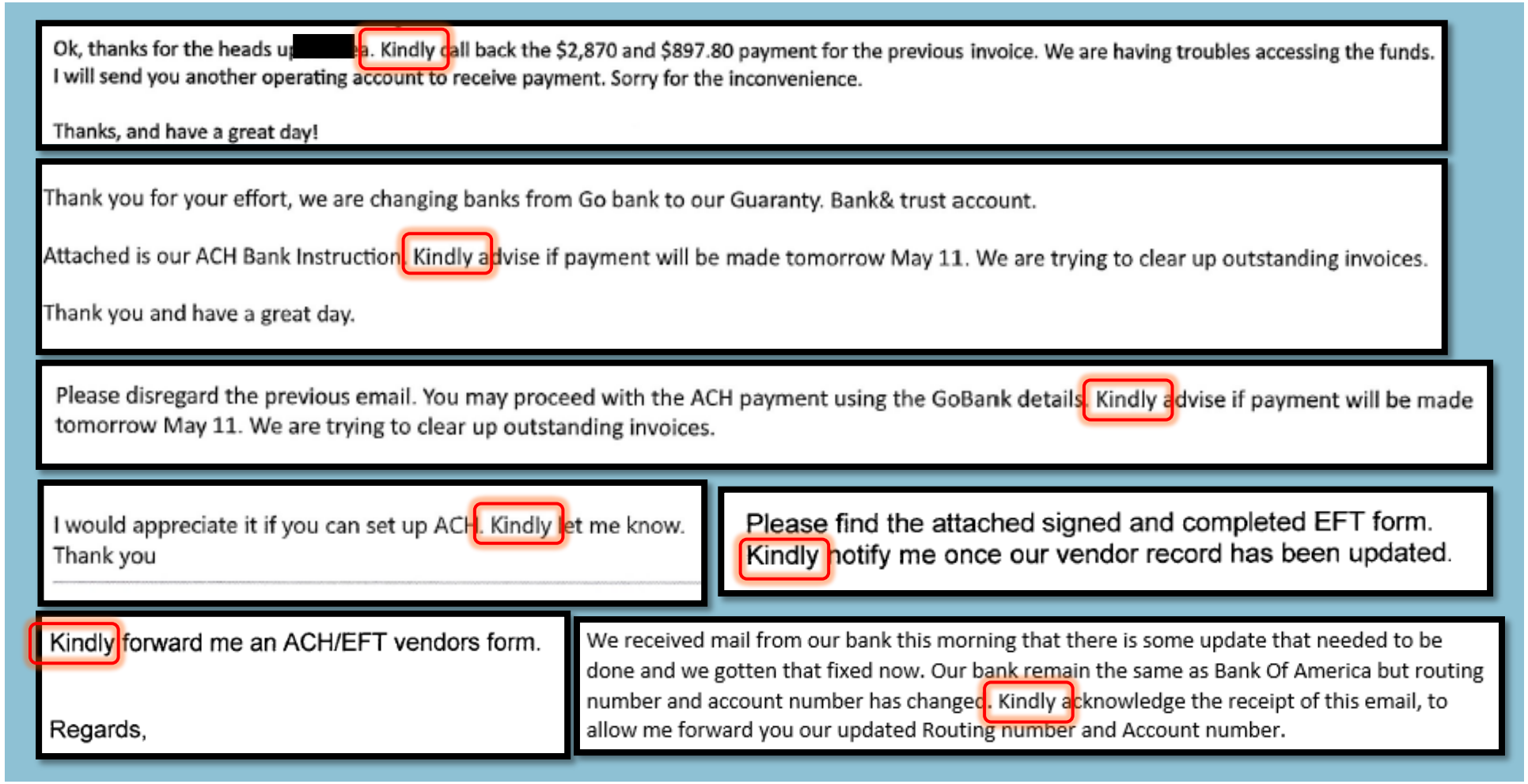
2. Request includes “kindly” or other language that seems atypical

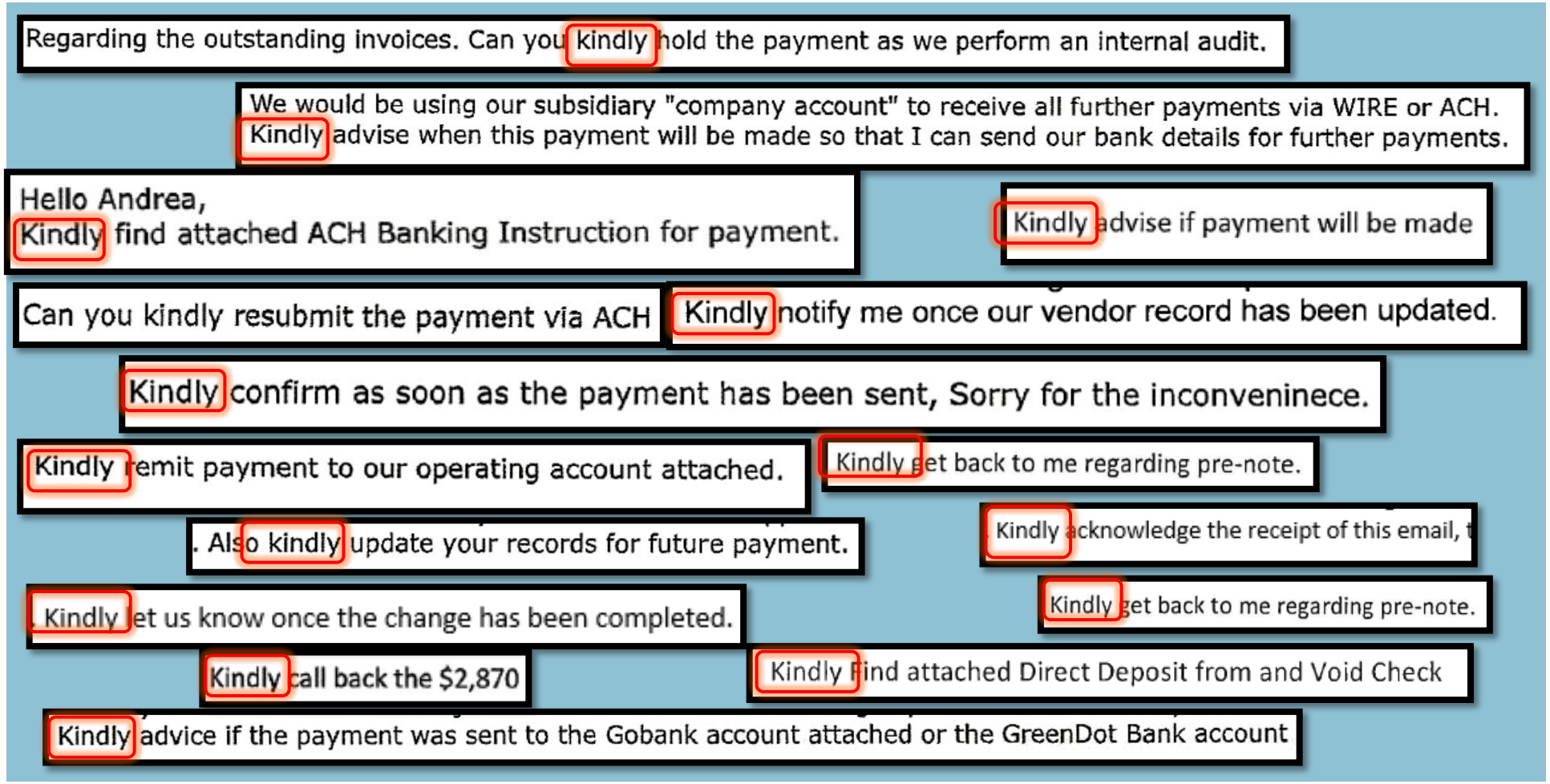
3. Provides a voided check that anyone could create, and/or a typed signature

4. Email address is not an exact match, or is an outside address when it should be internal

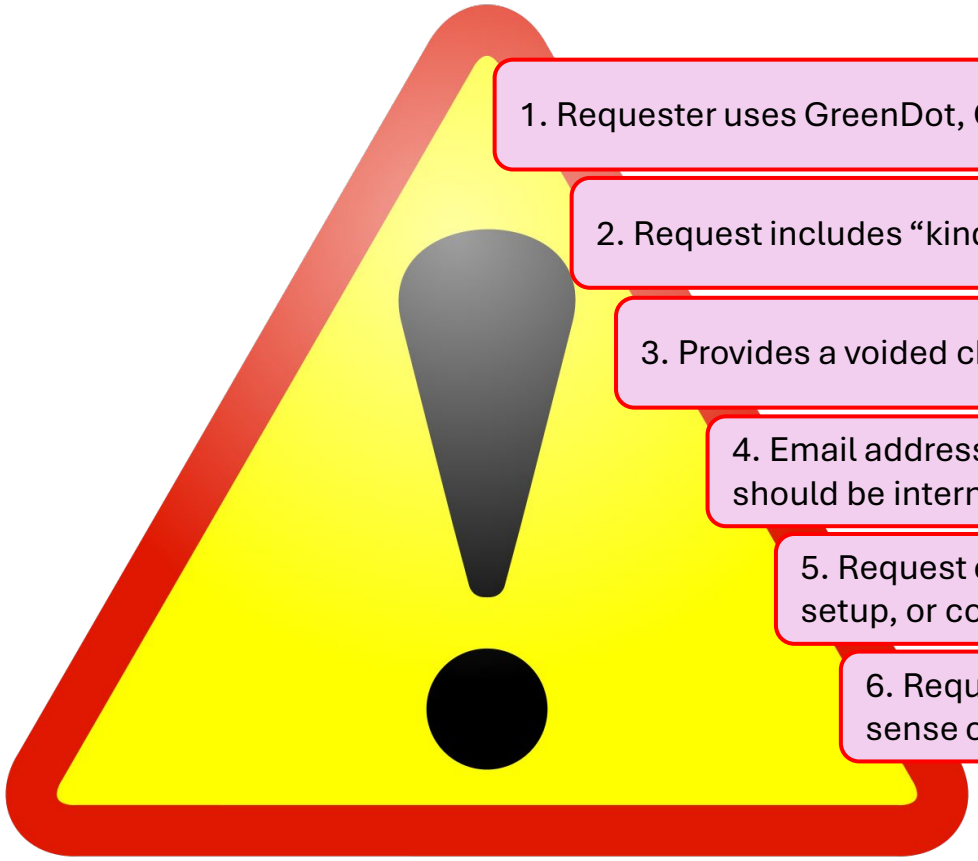
5. Request comes via email when you have a different method setup, or comes to the wrong department

6. Request comes in close to payment date and/or creates a sense of urgency


Ok, thanks for the heads up [redacted]a. Kindly call back the $2,870 and $897.80 payment for the previous invoice. We are having troubles accessing the funds. I will send you another operating account to receive payment. Sorry for the inconvenience.
Thanks, and have a great day!
Thank you for your effort, we are changing banks from Go bank to our Guaranty. Bank& trust account.
Attached is our ACH Bank Instruction. Kindly advise if payment will be made tomorrow May 11. We are trying to clear up outstanding invoices.
Thank you and have a great day.
Please disregard the previous email. You may proceed with the ACH payment using the GoBank details. Kindly advise if payment will be made tomorrow May 11. We are trying to clear up outstanding invoices.
I would appreciate it if you can set up ACH. Kindly let me know.
Thank you
Please find the attached signed and completed EFT form.
Kindly notify me once our vendor record has been updated.
Kindly forward me an ACH/EFT vendors form.
Regards,
We received mail from our bank this morning that there is some update that needed to be done and we gotten that fixed now. Our bank remain the same as Bank Of America but routing number and account number has changed. Kindly acknowledge the receipt of this email, to allow me forward you our updated Routing number and Account number.

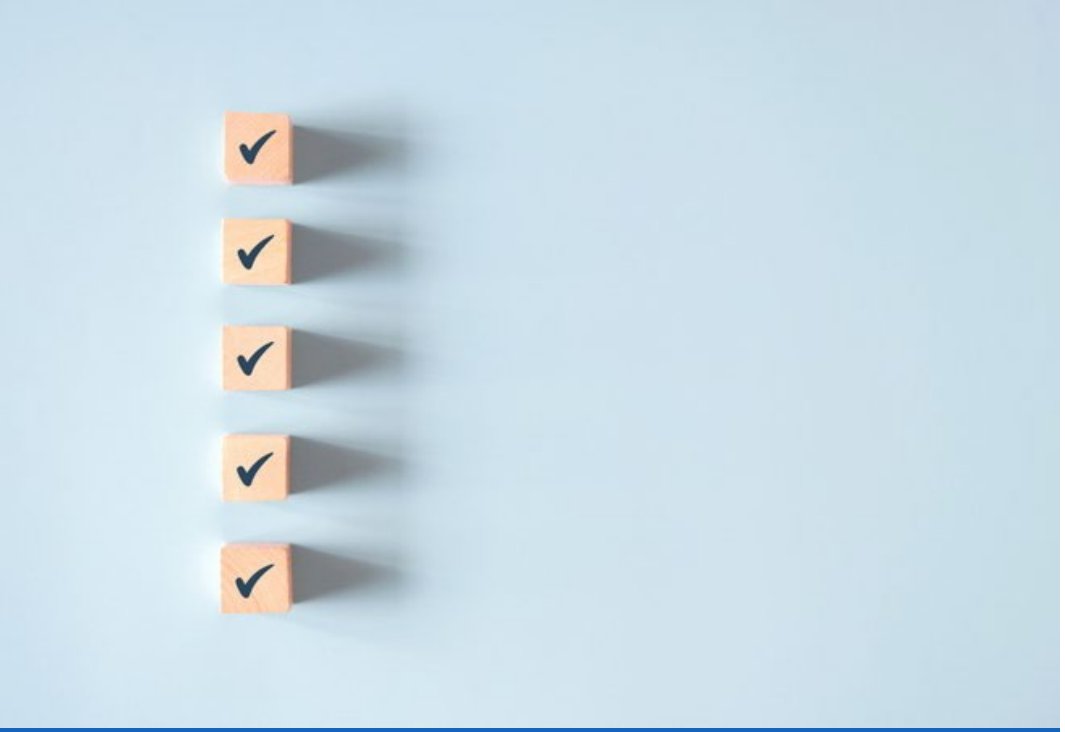

Regarding the outstanding invoices. Can you kindly hold the payment as we perform an internal audit.
We would be using our subsidiary "company account" to receive all further payments via WIRE or ACH.
Kindly advise when this payment will be made so that I can send our bank details for further payments.
Hello Andrea,
Kindly find attached ACH Banking Instruction for payment.
Kindly advise if payment will be made
Can you kindly resubmit the payment via ACH
Kindly notify me once our vendor record has been updated.
Kindly confirm as soon as the payment has been sent, Sorry for the inconveninece.
Kindly remit payment to our operating account attached.
Kindly get back to me regarding pre-note.
. Also kindly update your records for future payment.
Kindly acknowledge the receipt of this email,
Kindly let us know once the change has been completed.
Kindly get back to me regarding pre-note.
Kindly call back the $2,870
Kindly Find attached Direct Deposit from and Void Check
Kindly advice if the payment was sent to the Gobank account attached or the GreenDot Bank account

Fraud warning signs



1. Requester uses GreenDot, GoBank, Walmart or Meta
2. Request includes “kindly” or other language that seems atypical
3. Provides a voided check that anyone could create, and/or a typed signature
4. Email address is not an exact match, or is an outside address when it should be internal
5. Request comes via email when you have a different method setup, or comes to the wrong department
6. Request comes in close to payment date and/or creates a sense of urgency

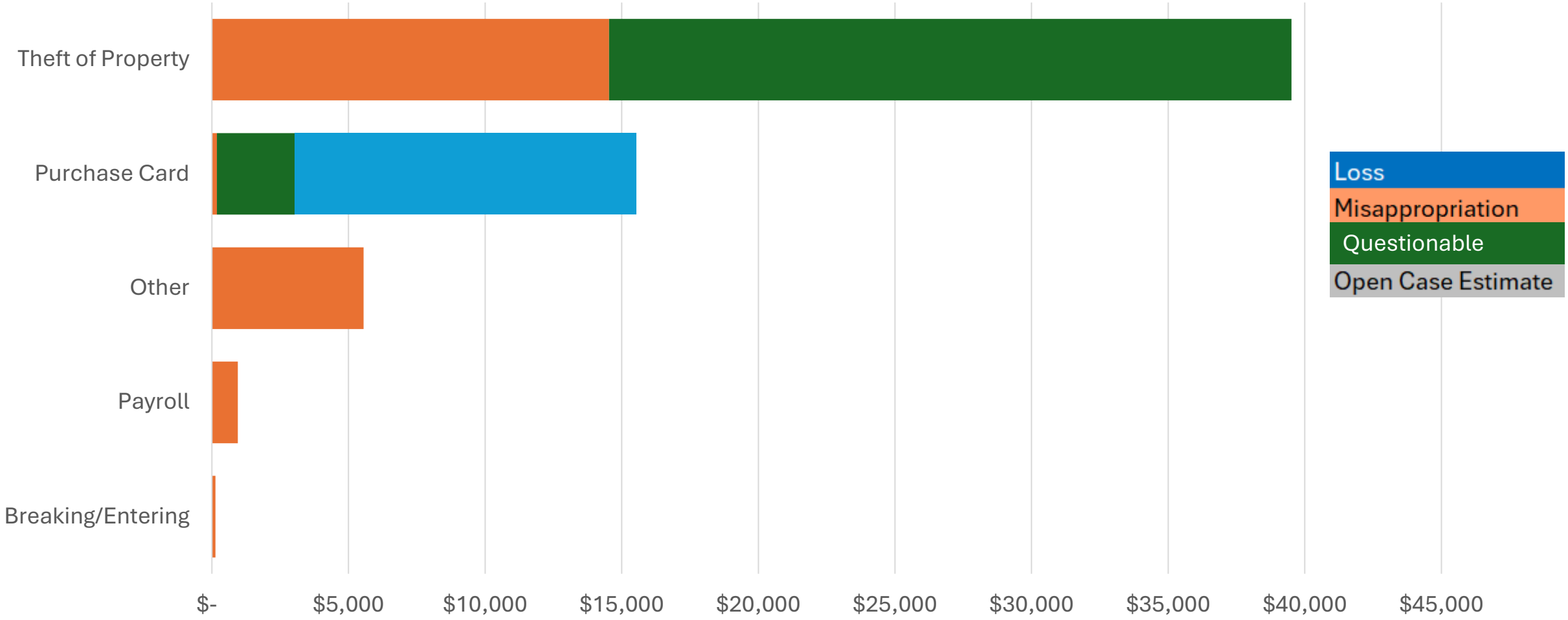
GreenDot Bank



What can you do?

- Don’t trust email. Literally, ever.
- Assume it’s a scam until you’re proven otherwise
- Request that employees make changes in person
- Vendors:
  - Confirm via video call you initiate
  - Provide contractors and vendors with a security key or passphrase they must provide for any contact for bank changes (do not send via email)

Most costly fraud schemes



Fraud-prevention resource for elected officials and appointed board members

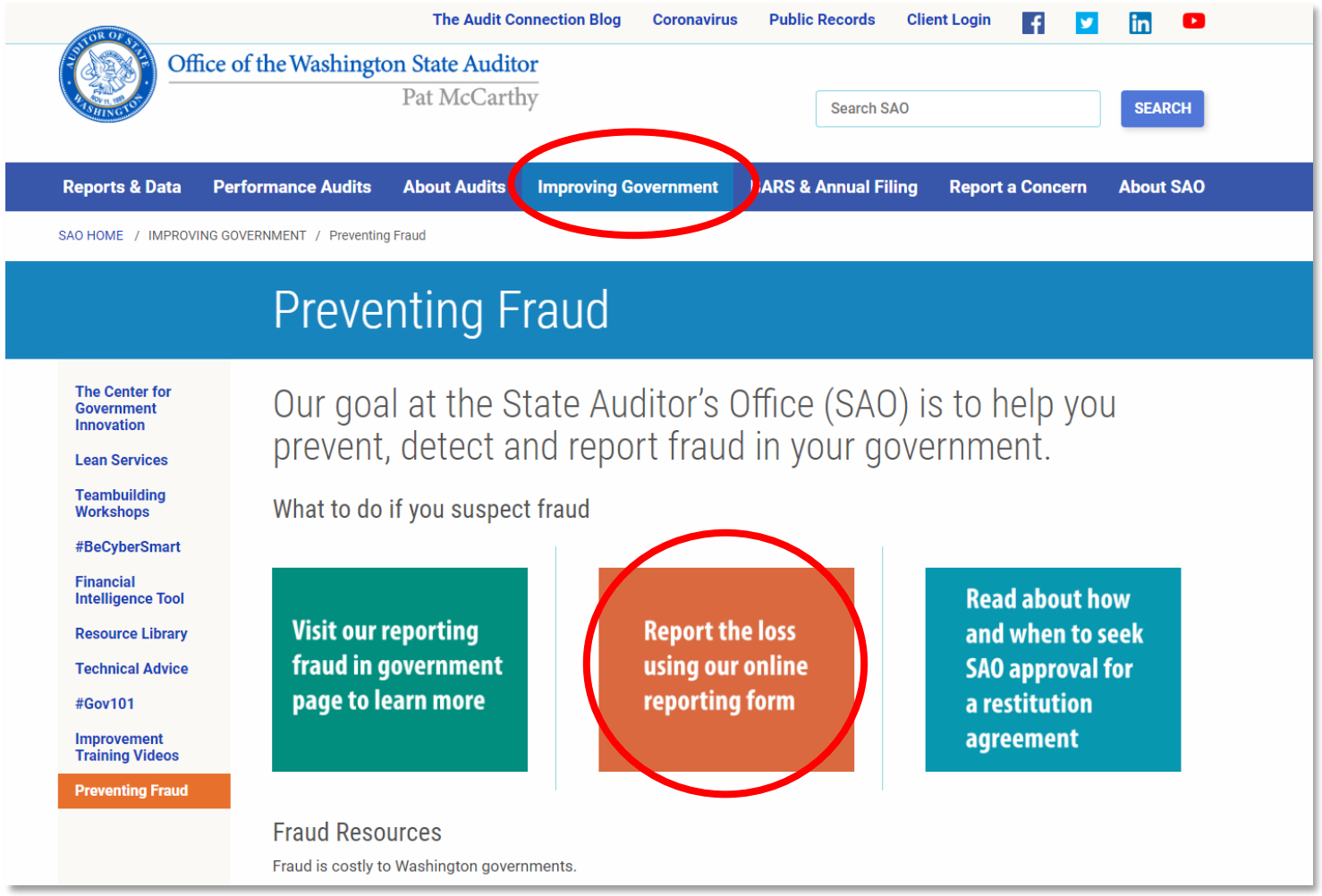
Key theme: Preventing fraud begins at the top

- Elected officials and appointed boards:
  - Have a duty to understand their government's operations
  - Play a key role in fighting fraud
  - Have a responsibility to demonstrate a commitment to preventing, detecting and responding to fraud—which are the three main sections of the guide

Fraud prevention resource library

Reporting fraud or loss

- Remember to report any known or suspected instances of fraud or loss to SAO (RCW 43.09.185)
- Easiest to do this through SAO's website



Support for Ports at SAO

Ports always have support when working with SAO during an audit.

People you can contact:

- Port program manager and subject matter experts (SMEs)
- Local audit staff
- Client HelpDesk
- And more …

Plus internal guidance:

- Planning guides
- Level of reporting

Questions?

Please feel free to contact me at any time.

Deena Garza
Port Program Manager
Deena.Garza@sao.wa.gov
(360) 594-0571

Office of the Washington State Auditor

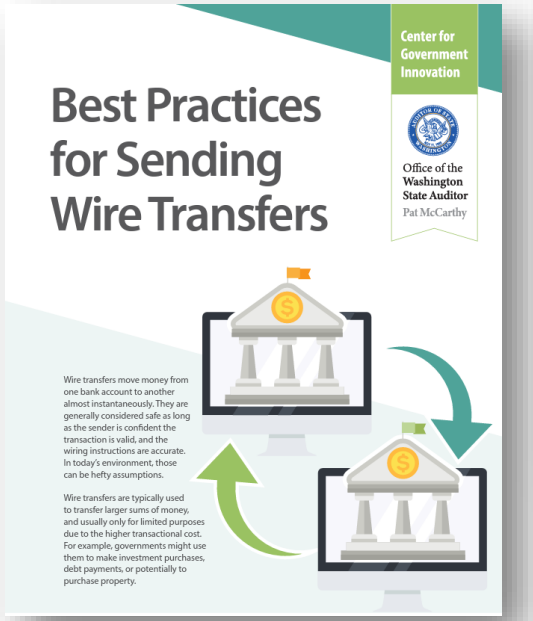
SAO resources from the Center of Government Innovation

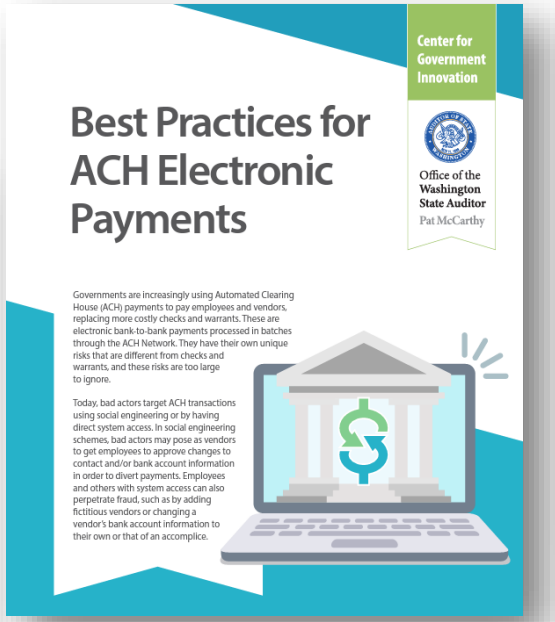
Scott Woelfle,
Director of Quality Assurance and Innovation

The Center for Government Innovation

- **Resource Library** with tools, checklists and other resources that provide you ways to improve internal controls, compliance and other areas
- **Cyber checkups** to assess your government's vulnerability to common cybersecurity threats
- **Financial Intelligence Tool (FIT)** to help you monitor your government's financial health
- **Teambuilding workshops** to help you strengthen your team, increase trust and promote workplace harmony
- **Customized Lean facilitations & trainings** to help you improve how work gets done

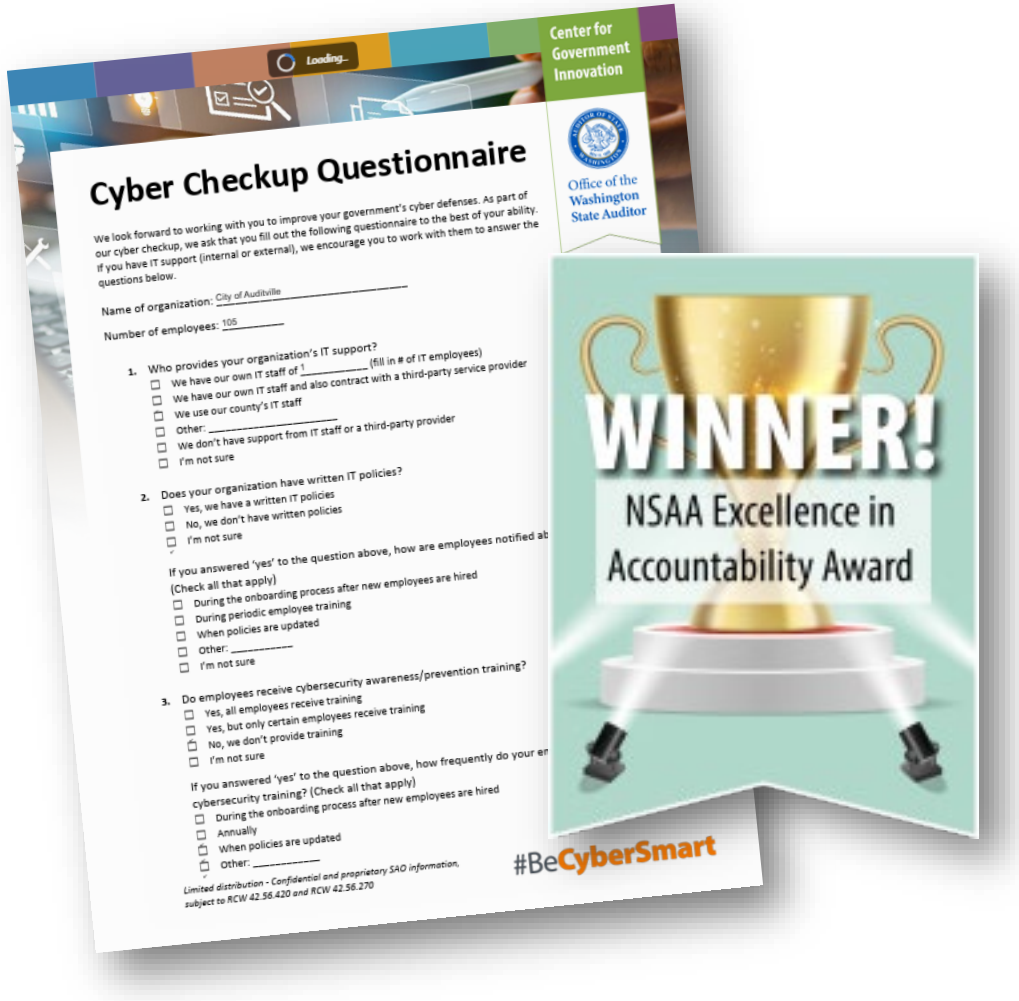
Resources for ports



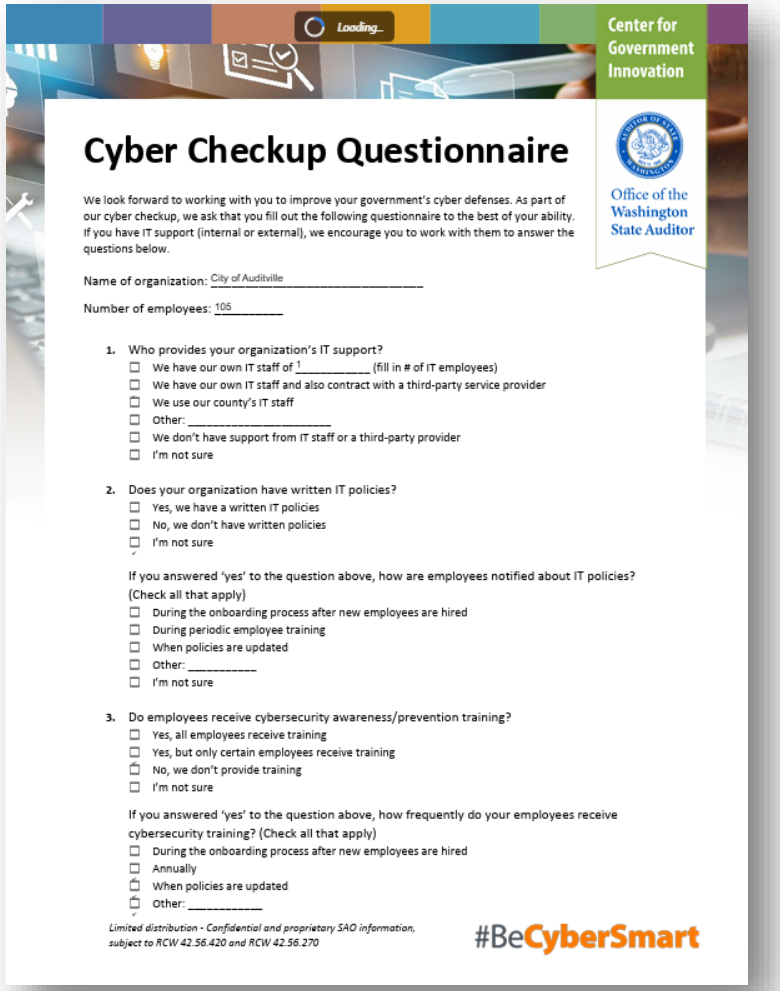


A multi-point inspection for a government's cyber program

- ✓ Completed remotely
- ✓ Ports answer a 20-question survey about security policies and practical measures
- ✓ SAO produces a summary of your results and recommendations, including easy and low-cost next steps



Cyber checkups



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.

Name of organization: City of Auditville

Number of employees: 105

1. Who provides your organization's IT support?
   - ☐ We have our own IT staff of 1 _____ (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

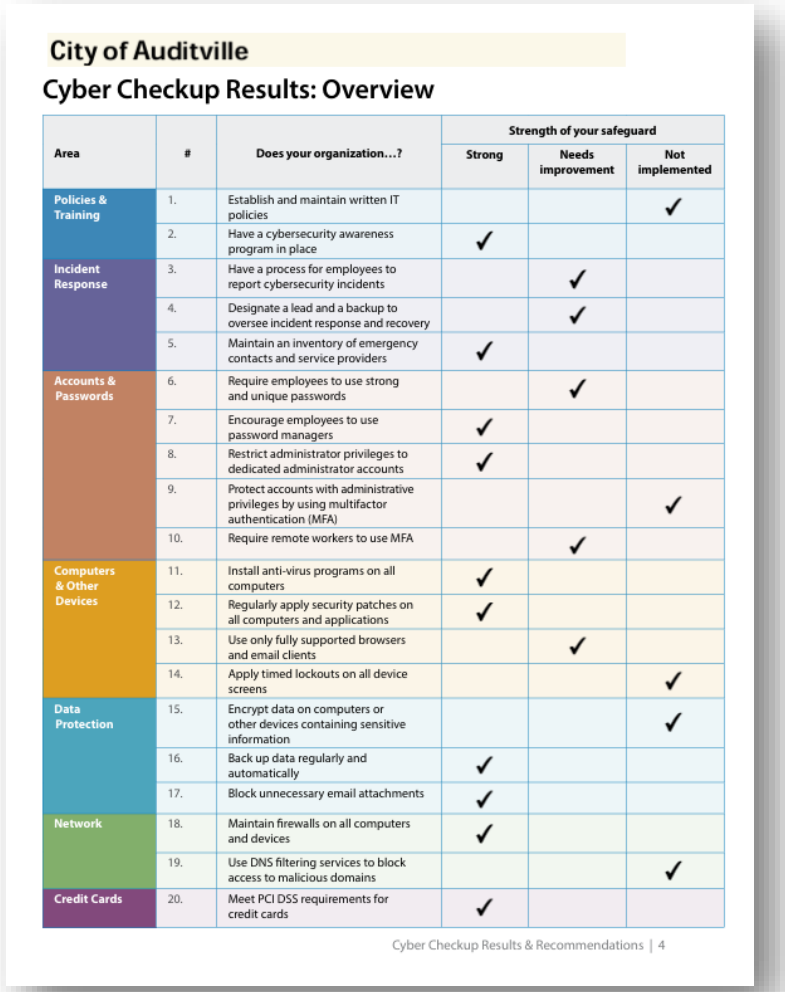
   If you answered 'yes' to the question above, how are employees notified about IT policies? (Check all that apply)
   - ☐ During the onboarding process after new employees are hired
   - ☐ During periodic employee training
   - ☐ When policies are updated
   - ☐ Other: _____
   - ☐ I'm not sure

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



City of Auditville

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	✓		

Policies & Training

Safeguard 2: Have a cybersecurity awareness program in place

About this safeguard

A cybersecurity awareness program trains employees to be mindful of cybersecurity risks as they perform their daily tasks. Employees should be aware of common fraud and phishing schemes, as well as basic techniques bad actors use to trick unsuspecting employees.

Why this safeguard is important

People are often an organization's weakest link. Hackers focus on taking advantage of human nature to gain access to your government's networks and sensitive information. Through social engineering techniques like phishing and smishing (using text messages instead of email), they manipulate human behaviors to gain access to login credentials and networks that, if improperly used, could reveal critical data or otherwise harm your government. While you may have put technical solutions in place to reduce the likelihood malicious activities will succeed, your overall security requires an embedded culture of cybersecurity awareness to be truly effective. With regular training, people can become your government's first line of defense.

What we observed during the checkup

Your organization has a cybersecurity awareness program in place.

Our recommendations

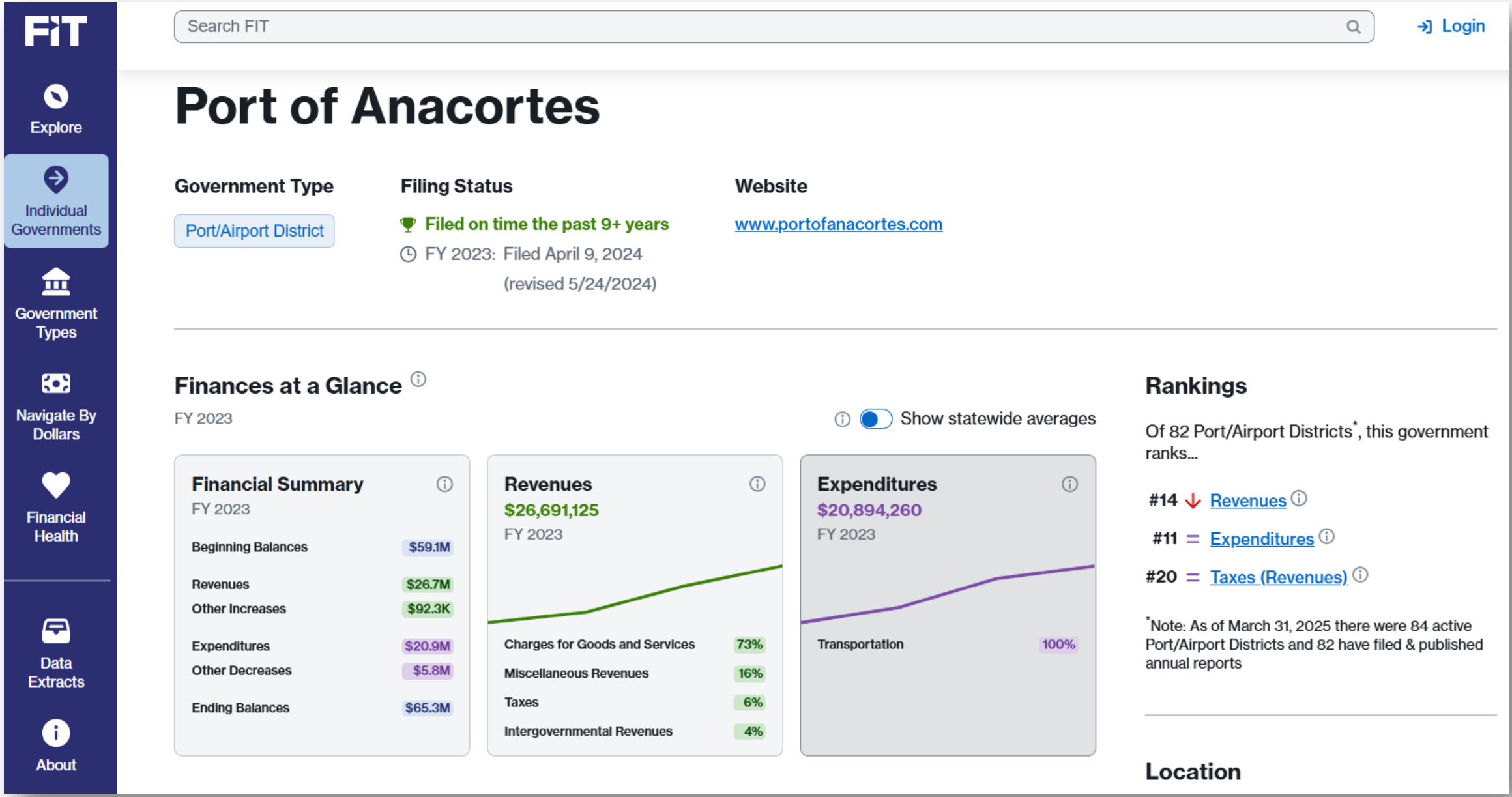
- Develop and implement a policy requiring employees to take regular cybersecurity awareness training. You can find links to example policies in the Resources section below.
- Create a cybersecurity awareness program that fits your government's needs. Awareness encompasses everything from a formal security awareness training program to a monthly email with cybersecurity tips, each designed to influence employees' behavior. There are many low-cost and free resources (see Resources below) to help you get started. You'll find tools for delivering training modules, assessments, and newsletters to keep employees engaged.
- Conduct training as part of onboarding for new employees and then annually for all staff.
- Review your training program and its associated policy annually to ensure your program is keeping up with evolving types of cyberattacks.

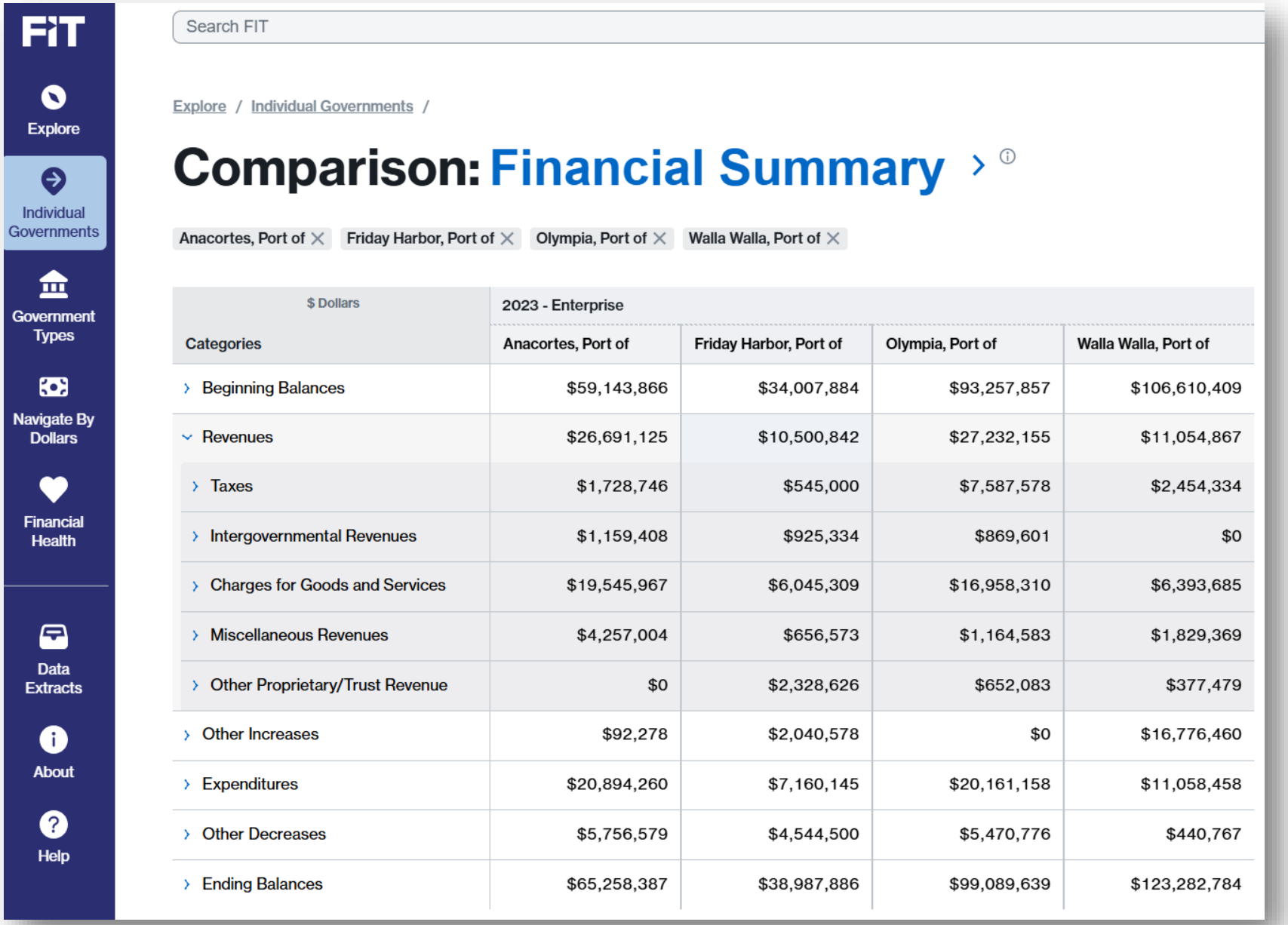
Resources and references you can use

- The National Institute of Standards and Technology (NIST) provides a sample template you can use to develop your own security awareness training policy.
- SAO's "People matter in cybersecurity" offers advice for starting an awareness program.
- Infosec Institute offers a free toolkit and training resources you can download.
- NIST provides a list of free and low-cost trainings you can use today to start your program.

This safeguard supports CIS Control 14.1

Your data—the Financial Intelligence Tool (FIT)


FIT
Search FIT
Login
Explore
Individual Governments
Government Types
Navigate By Dollars
Financial Health
Data Extracts
About
Port of Anacortes
Government Type
Port/Airport District
Filing Status
Filed on time the past 9+ years
FY 2023: Filed April 9, 2024
(revised 5/24/2024)
Website
www.portofanacortes.com
Finances at a Glance
FY 2023
Show statewide averages
Financial Summary
FY 2023
Beginning Balances $59.1M
Revenues $26.7M
Other Increases $92.3K
Expenditures $20.9M
Other Decreases $5.8M
Ending Balances $65.3M
Revenues
$26,691,125
FY 2023
Charges for Goods and Services 73%
Miscellaneous Revenues 16%
Taxes 6%
Intergovernmental Revenues 4%
Expenditures
$20,894,260
FY 2023
Transportation 100%
Rankings
Of 82 Port/Airport Districts*, this government ranks...
#14 Revenues
#11 Expenditures
#20 Taxes (Revenues)
*Note: As of March 31, 2025 there were 84 active Port/Airport Districts and 82 have filed & published annual reports
Location



Compare side by side

Questions?

Office of the Washington State Auditor

Lean for ports: An overview

01: Lean Methodology

- What is Lean?
- How does Lean work?

02: Lean in Real Life

- Improvement projects

03: Services & Resources

- Free onsite and online

Joanna Bailey, Lean Specialist

What is Lean?

Process improvement methodology

Re-assess yesterday's logic to:

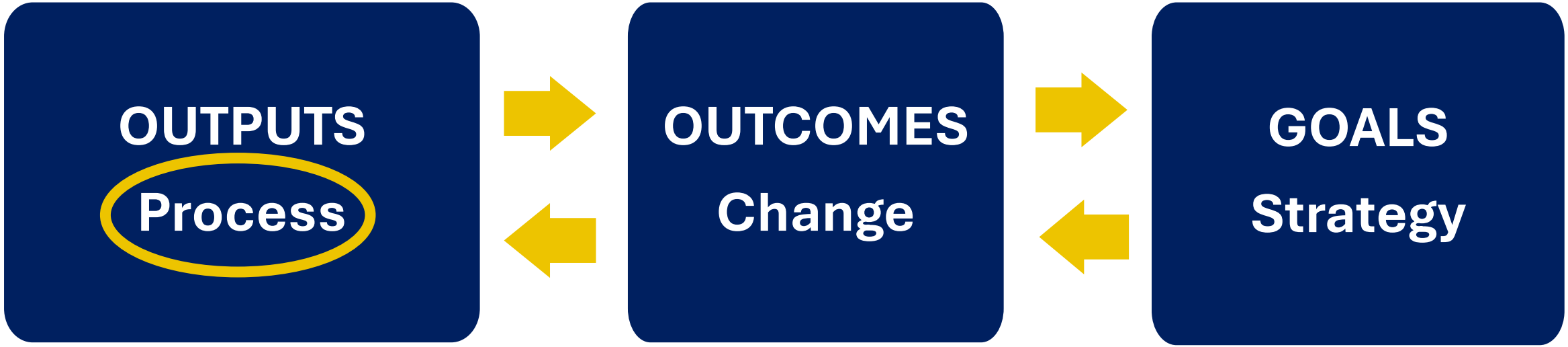
- Build a **shared understanding** of process challenges & opportunities.
- Remove process waste to use **current resources** more effectively.
- Mitigate risk through **incremental** changes.

How does Lean work?

Purpose-driven principles

1. **Fix process, not people**
   Provide effective tools for staff success.
2. **Make work visible**
   See to understand; understand to improve.
3. **Eliminate process waste**
   Increase capacity to do important work.
4. **Go slow to go fast**
   Small changes to mitigate change risk.

Principle: Fix process, not people



Principle: Eliminate process waste

Motion

- Treasure hunting
- Duplicate data entry

Rework

- Incomplete or inaccurate work
- Passing errors downstream

Waiting

- Signatures
- Single user access

Underutilized resources/skills

- Unused software functionality
- Task distribution

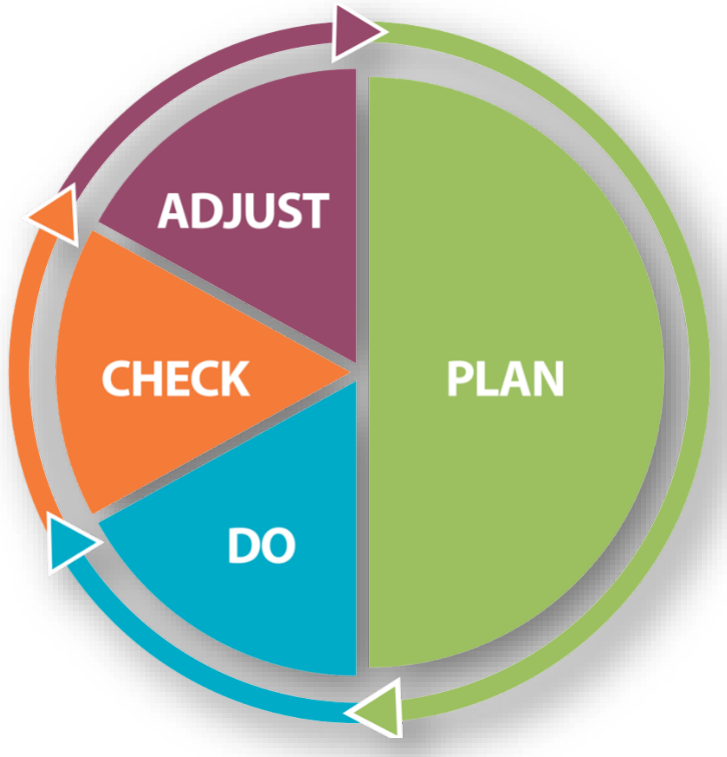
Overproduction/processing

- Parallel file systems
- Digital-to-print; print-to-digital

Principle: Go slow to go fast

4 steps to a better process:

- Plan – prepare for the change
- Do – trial improvements
- Check – to assure improvement
- Adjust – lock in to standardize



Lean in real life

Credit card reconciliation

Case Study #1: Current state conditions

1. 54 credit cards: employees + commissioners
2. Reconciliation: 3 finance staff
3. Process challenges:

    ✓Late submittals, coding errors, missing entries and receipts

    ✓Stressful reconciliation, staff burnout

Lean in real life cont.

Credit card reconciliation cont.

Root causes:

1. Outdated cardholder agreement and procurement policy.
2. No expectation for cardholder to record or reconcile their activity prior to hand-off.
3. Departments log transactions and match receipts after receival of statement.
4. Unclear expectations for supervisory review.

Lean in real life cont.

Credit card reconciliation cont.

Action plan: Strengthen internal controls

1. Regularly assess # of cardholders to business need. Metric: dept justifications
2. Cardholder records and reconciles own activity against statement before handoff. Metric: performance evaluation
3. Establish expectations for supervisor review. Metric: # or % of send-backs

Lean in real life cont.

Credit card reconciliation cont.

Action plan: Timely submittals to finance

1. Cardholders record transactions on ongoing basis. Metric: % compliance; % change in timely submittals

2. Packet: receipts are in statement transaction order. Metric: % compliance

3. Directors provide Finance with an assigned backup approver and activate “out of office” reply before leaving. Metric: % compliance; % change in rework by Finance

Lean in real life cont.

Tenant turnover

Case Study #2: Current state conditions

1. Lease revenue = 72% operating budget
2. Unclear standard of quality, roles and responsibilities
3. IMPACT:
   - ✓Frustrated tenants
   - ✓Staff burn-out
   - ✓Turnover delays = loss of revenue

Lean in real life cont.

Tenant turnover cont.

Root causes:

1. Task over-reach between teams
2. “Turn-key ready” quality was subjective
3. 60% of work orders were not logged (un-trackable)
4. Outdated, incomplete and underutilized checklists

Lean in real life cont.

Tenant turnover cont.

Action plan: Tenant-out process

1. Update checklist to deliver newly standardized quality. Metric: walk-through, feedback
2. FacOps logs all work orders, procures bids/cost estimates for approval, plans and executes site work. Metric: weekly reports, dashboard accountability
3. Real Estate communicates with tenant. Metric: customer & staff feedback
4. Eliminate staff's 2nd quality walk-through. Metric: walk-through, feedback

Lean in real life cont.

Tenant turnover cont.

Action plan: Tenant-in process

1. Update checklist to deliver newly standardized quality. Metric: walk-through, feedback
2. Real Estate communicates with tenant; sends improvement site requests to FacOps. Metric: customer & staff feedback
   - FacOps logs and tracks all work orders, procures bids/cost estimates for approval, plans and executes site work. Metric: weekly reports, dashboard accountability, staff feedback

Lean services: Easy

Customized Service: 1 click to start conversation

- ✓ Training workshops
- ✓ Facilitated improvement projects

Self-guided online learning:

- ✓ Lean project charter tools
- ✓ Process improvement webinar

Questions?

Office of the Washington State Auditor

Information

Scott Woelfle
Director of Quality Assurance & Innovation

Joanna Bailey
Lean Specialist

Center@sao.wa.gov

(564) 999-0818

Website: www.sao.wa.gov
X (formerly known as Twitter): www.X.com/WaStateAuditor
Facebook: www.facebook.com/WaStateAuditorsOffice