



# Internal controls: What they are and why they're important

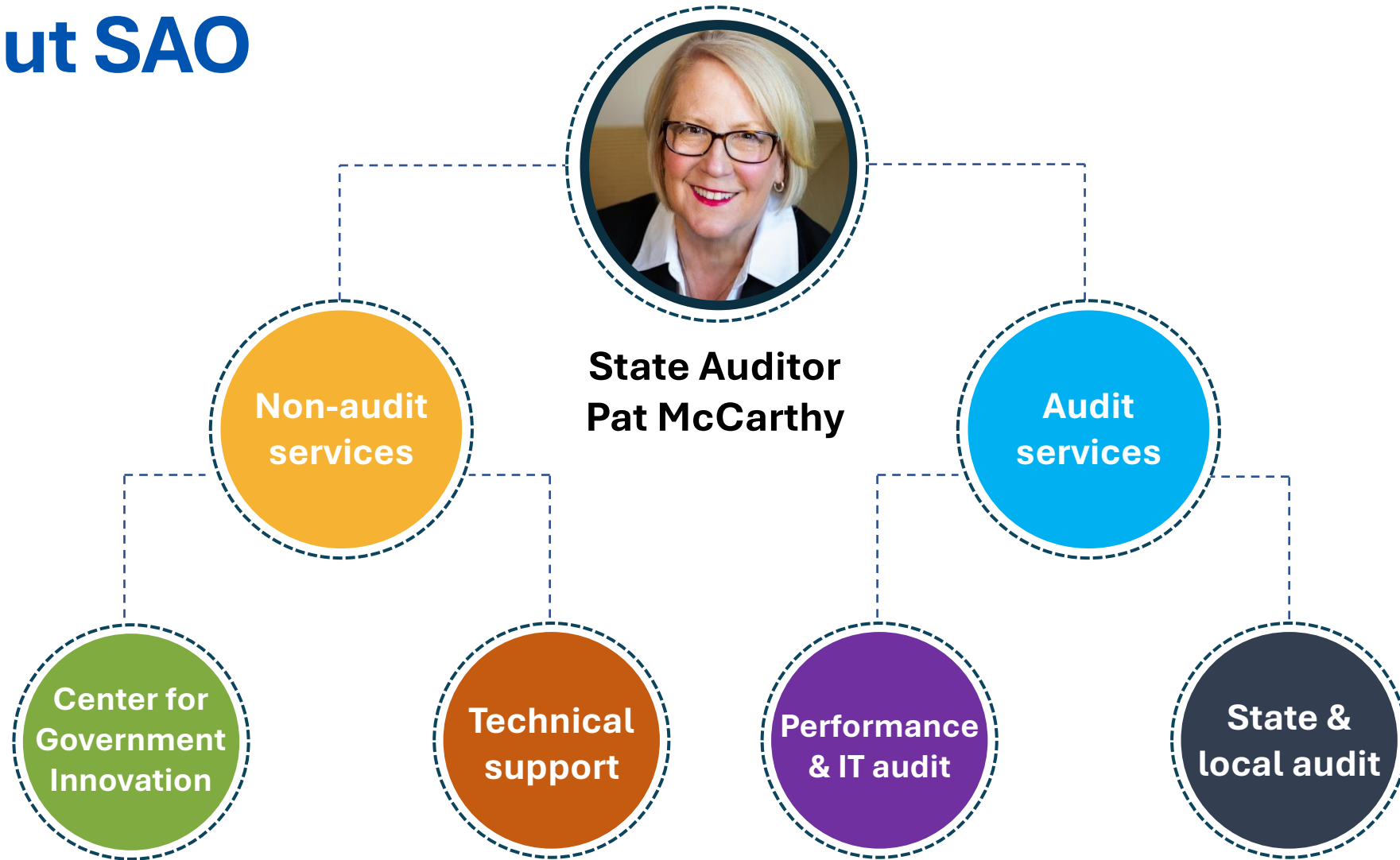
Niles Kostick, Manager  
Center for Government Innovation



# Sign up for our newsletter



# About SAO





# Center for Government Innovation

## No-cost Center services



Office of the Washington State Auditor

The Audit Connection Blog Coronavirus Public Records Client Login

Office of the Washington State Auditor  
Pat McCarthy

Search SAO

Reports & Data Performance Audits About Audits Improving Government BARS & Annual Filing Report a Concern About SAO

SAO HOME / IMPROVING GOVERNMENT / The Center for Government Innovation

## The Center for Government Innovation

**The Center for Government Innovation**

- Lean Services
- Teambuilding Workshops
- #BeCyberSmart
- Financial Intelligence Tool
- Resource Library
- Technical Advice
- #Gov101
- Improvement Training Videos
- Preventing Fraud

### EFFICIENCY TOOLBOX

Access the knowledge and resources to help your local government innovate and improve.

Helping local governments help the people they serve

We have resources to help local governments throughout Washington work better. We offer tools and services to help you solve problems and improve operations. Our team is available by phone, online or in person to offer assistance at no additional cost.

**Contact Us:**  
 564-999-0818  
 center@sao.wa.gov

**Lean Services**

We help you improve how work gets done. Whether it's purchasing, payroll, or any other area, Lean services can help your government optimize efficiency, quality and customer service.

[Find out more »](#)

**Teambuilding Workshops**

We offer engaging and interactive CliftonStrengths workshops to help strengthen your team, increase trust and productivity, and promote workplace harmony and employee satisfaction.

[Find out more »](#)

**#BeCyberSmart**

Local governments are attractive targets for cyber criminals. That's why we created the #BeCyberSmart program, which includes free checkups, resources and training, to help governments improve their overall cyber health.

[Find out more »](#)

**Financial Intelligence Tool**

Developed by the State Auditor's Office (SAO), the interactive Financial Intelligence Tool (FIT) gives you the data you need to help your government make better business decisions and improve its financial health.

[Financial Intelligence Tool »](#)

**Resource Library**

We provide a variety of free guides, checklists, and best practices to help governments improve internal controls, grants management, procurement practices, financial reporting, operations, technology and more.

[Find out more »](#)

**Technical Advice**

Connect with the Center's experts in Washington government operations to get answers to your questions about internal controls, procurement, financial reporting, cybersecurity and more.

[Find out more »](#)

4

# Resource Library

## Coming soon! Updated:

- ✓ Segregation of Duties Guide
- ✓ Change Order Best Practice
- ✓ Bank Reconciliations Best Practice
- ✓ Responsible Bidder Checklist

The screenshot shows the website for the Office of the Washington State Auditor, Pat McCarthy. The page is titled "Resource Library" and features a navigation menu with categories like "Reports & Data", "Performance Audits", "About Audits", "Improving Government", "BARS & Annual Filing", "Report a Concern", and "About SAO". A search bar is located in the top right corner. The main content area is divided into several sections:

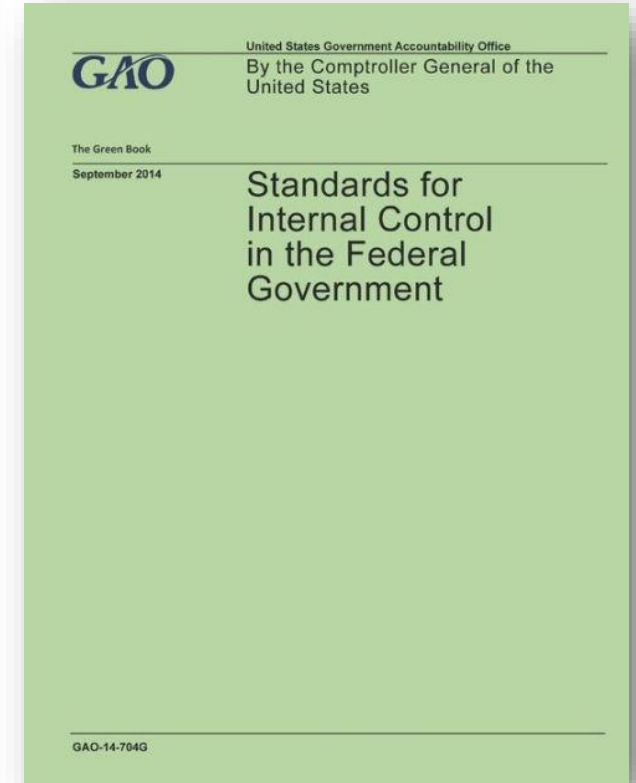
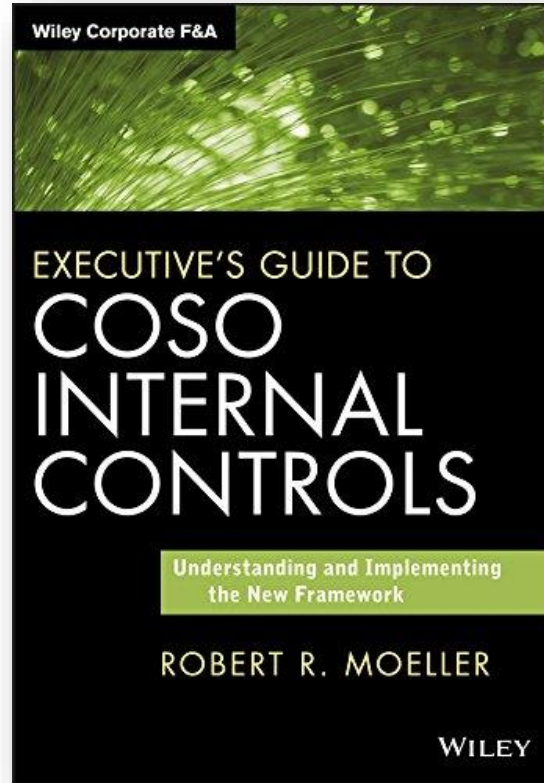
- Internal Controls:** Includes buttons for "ACCOUNTS PAYABLE", "CASH RECEIPTING", "PAYROLL", and "ASSETS".
- Compliance:** Includes buttons for "PROCUREMENT" and "FEDERAL FUNDS".
- Financial Reporting:** Includes buttons for "GAAP BASIS" and "CASH BASIS".
- Government Operations:** Includes buttons for "OPERATIONS", "LEAN SERVICES", "REVENUES", and "EXPENDITURES".
- Organizational Safeguards:** Includes buttons for "CYBERSECURITY", "TECHNOLOGY", and "FRAUD PREVENTION".

On the right side, there is a "Featured resource" section with a graphic titled "Trust, but verify: A guide for elected officials & appointed boards to prevent fraud". Below this, there is a "View/download PDF" link and a section titled "Want to know when SAO releases new resources?" with a small graphic titled "In the KNOW with SAO".





# Internal controls: The big picture





## Internal controls: The big picture

“To help us get what we want”





**What do you want?**

## **Internal controls: The big picture**





## Internal controls: The big picture (cont.)

**“To help us get what we want”**

### Some example objectives:

- ✓ Comply with state law and regulations
- ✓ Adhere to City policy
- ✓ Allow for efficient services and business continuity
- ✓ Ensure public funds are used appropriately
- ✓ Educate staff and reduce confusion





## Internal controls: The big picture (cont.)

### Leading causes of occupational fraud:

32%

Lack of internal controls

19%

Override of existing controls

18%

Lack of management review

8%

Poor tone at the top





## Internal controls: The big picture (cont.)

## The Fraud Triangle





## Internal controls: The big picture (cont.)

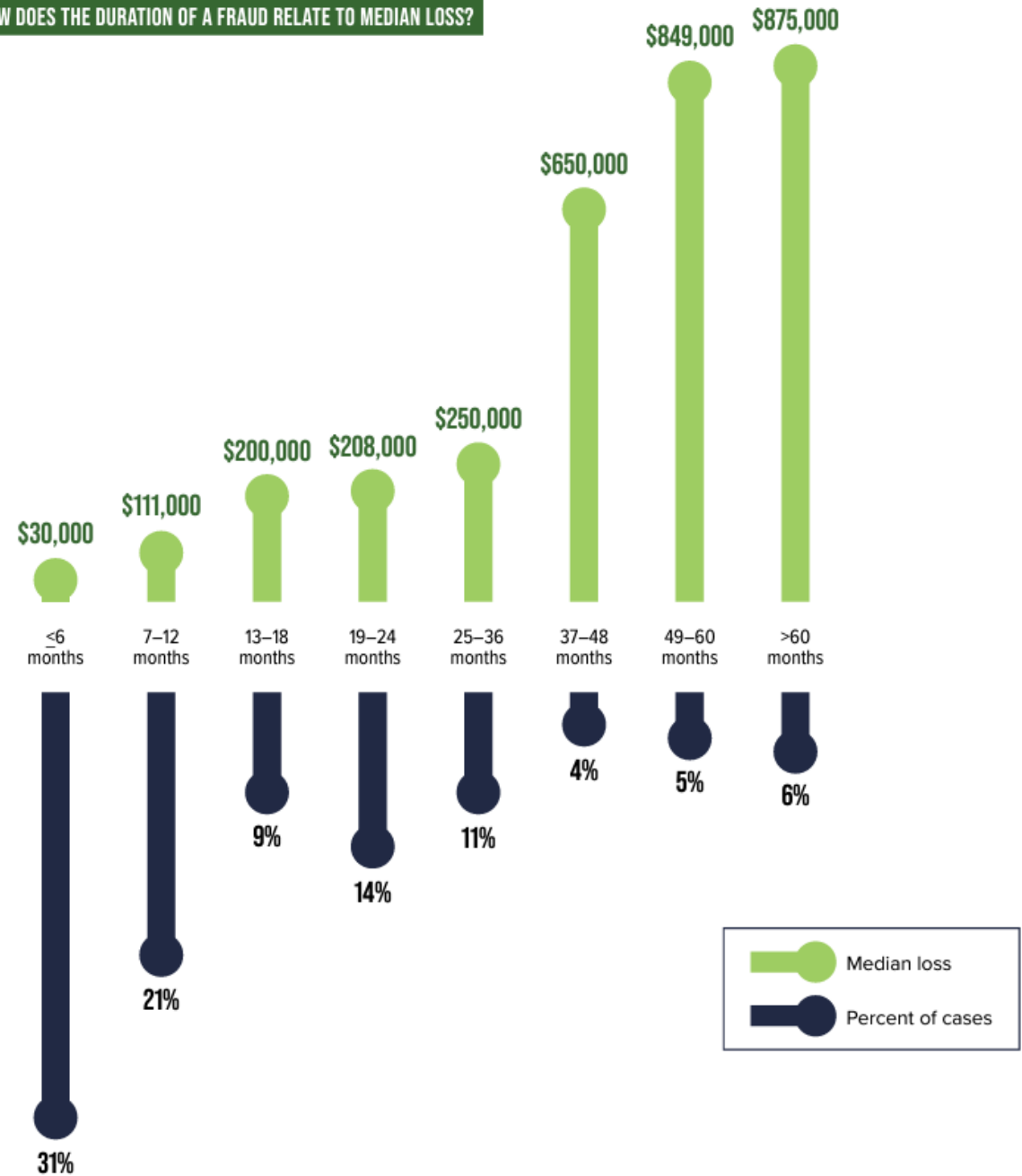
- **Faster detection often leads to smaller loss**
- **Fast detection relies on adequate controls**





# Internal controls: The big picture (cont.)

FIG. 7 HOW DOES THE DURATION OF A FRAUD RELATE TO MEDIAN LOSS?

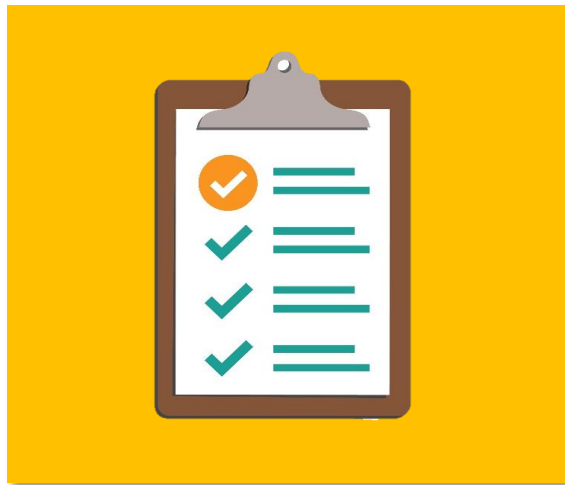


## Internal controls: The big picture (cont.)

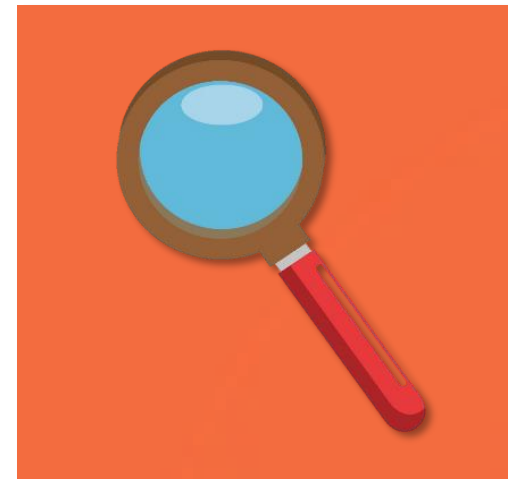
**THE LONGER** A  
FRAUDSTER HAS WORKED FOR AN  
ORGANIZATION, **THE MORE**  
**COSTLY** THE FRAUD.



# Internal controls: The big picture (cont.)



**Preventative**



**Detective**

# Three simple prevention & detection reviews you can implement now



**Review expenditures before approving**



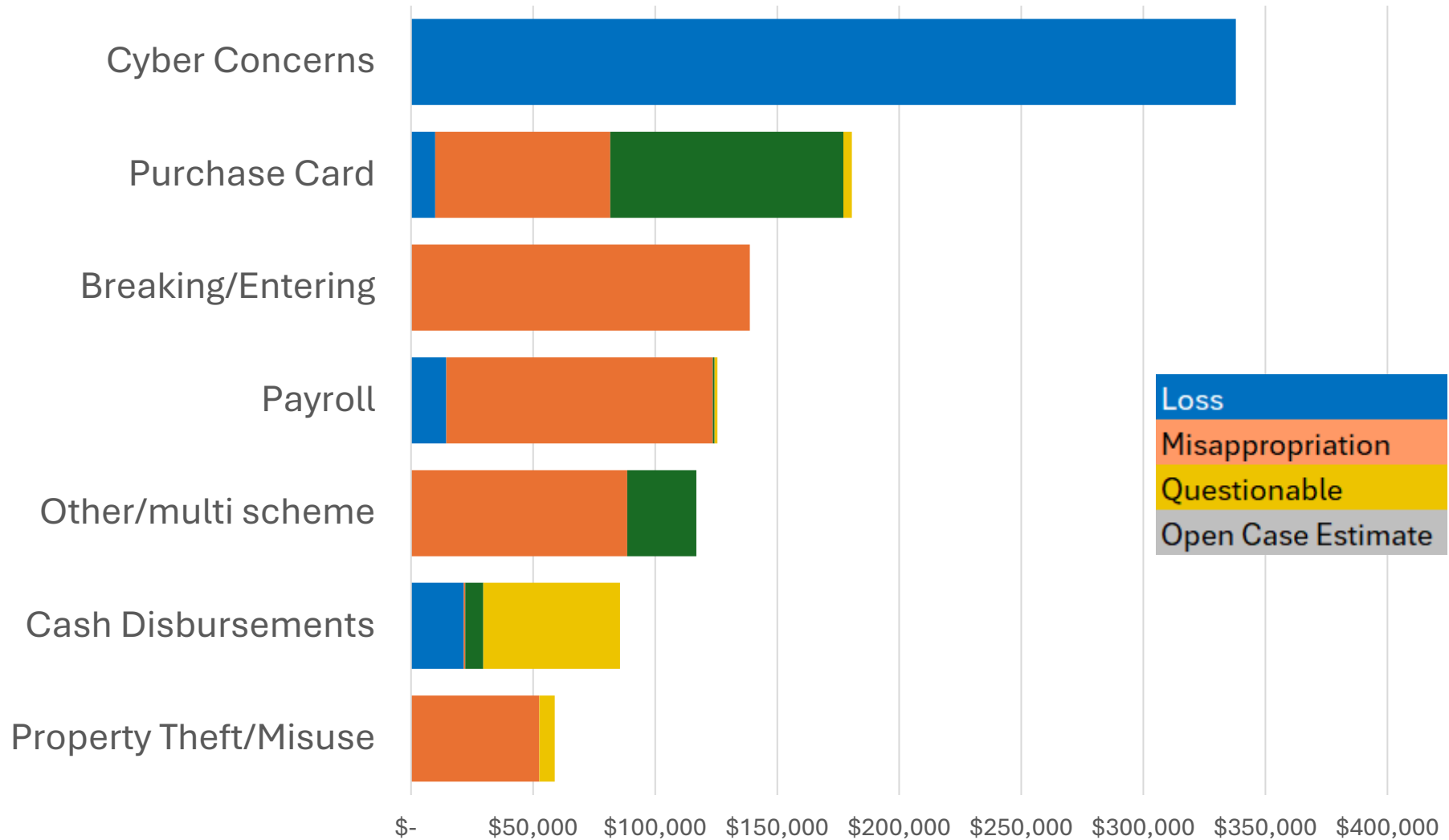
**Review the bank statements**



**Review payroll amounts**



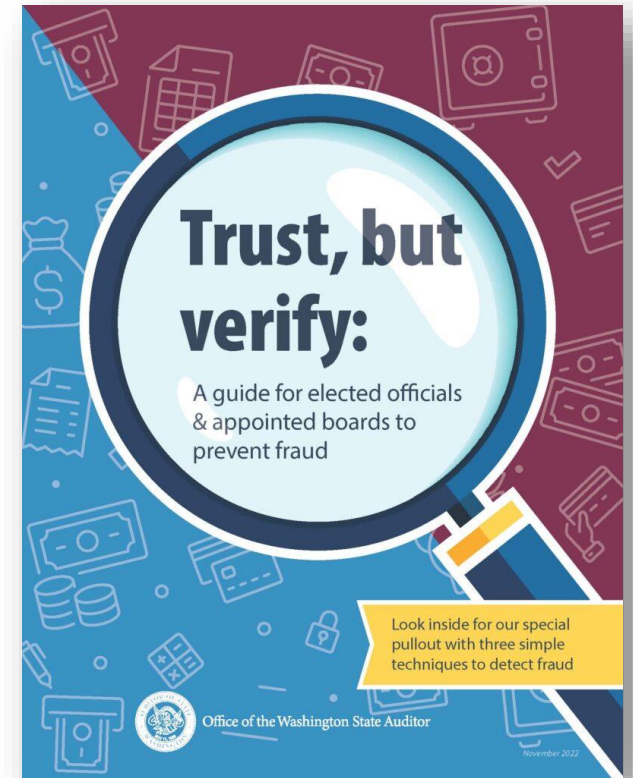
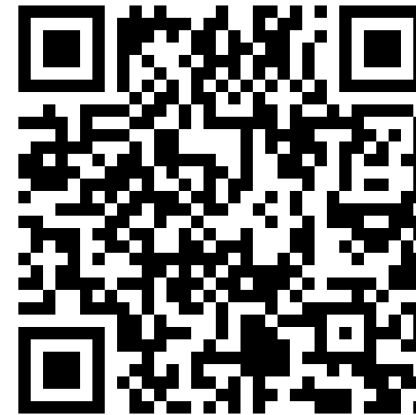
# Most costly fraud schemes



# Fraud prevention resource for elected officials & 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



# The intersection of policy and process

## Policy (What and why)

- High-level principles that set direction
- Ensures compliance, accountability, consistency
- **Example:** “All credit cards are for official business use only”

## Process (How)

- Step-by-step instructions and structure
- Provides clear execution methods for achieving the policy (how we meet our high-level goals)
- **Example:** Card holders will review their own statements before submitting them for payment

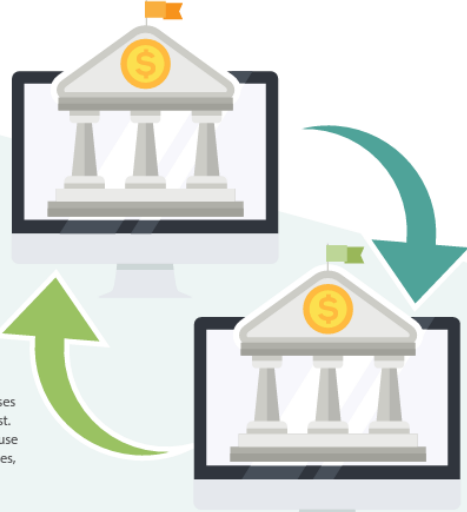


# Center resources

Center for Government Innovation

Office of the Washington State Auditor  
Pat McCarthy

## Best Practices for Sending Wire Transfers



Wire transfers move money from one bank account to another almost instantaneously. They are generally considered safe as long as the sender is confident the transaction is valid, and the wiring instructions are accurate. In today's environment, those can be hefty assumptions.

Wire transfers are typically used to transfer larger sums of money, and usually only for limited purposes due to the higher transactional cost. For example, governments might use them to make investment purchases, debt payments, or potentially to purchase property.


Center for Government Innovation

Office of the Washington State Auditor  
Pat McCarthy

## Best Practices for ACH Electronic Payments

Governments are increasingly using Automated Clearing House (ACH) payments to pay employees and vendors, replacing more costly checks and warrants. These are electronic bank-to-bank payments processed in batches through the ACH Network. They have their own unique risks that are different from checks and warrants, and these risks are too large to ignore.

Today, bad actors target ACH transactions using social engineering or by having direct system access. In social engineering schemes, bad actors may pose as vendors to get employees to approve changes to contact and/or bank account information in order to divert payments. Employees and others with system access can also perpetrate fraud, such as by adding fictitious vendors or changing a vendor's bank account information to their own or that of an accomplice.





## 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)

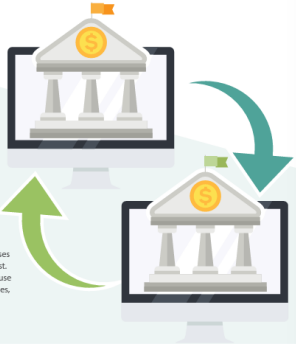


## Best Practices for Sending Wire Transfers

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

Wire transfers move money from one bank account to another almost instantaneously. They are generally considered safe as long as the sender is confident the transaction is valid, and the wiring instructions are accurate. In today's environment, those can be hefty assumptions.

Wire transfers are typically used to transfer larger sums of money, and usually only for limited purposes due to the higher transactional cost. For example, governments might use them to make investment purchases, debt payments, or potentially to purchase property.



## Best Practices for ACH Electronic Payments

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

Governments are increasingly using Automated Clearing House (ACH) payments to pay employees and vendors, replacing more costly checks and warrants. These are electronic bank-to-bank payments processed in batches through the ACH Network. They have their own unique risks that are different from checks and warrants, and these risks are too large to ignore.

Today, bad actors target ACH transactions using social engineering or by having direct system access. In social engineering schemes, bad actors may pose as vendors to get employees to approve changes to contact and/or bank account information in order to divert payments. Employees and others with system access can also perpetrate fraud, such as by adding fictitious vendors or changing a vendor's bank account information to their own or that of an accomplice.



## Reminders & best practices

- Robust policies that outline employee responsibilities, define controls over payee information, and review them annually
- Educate staff on social engineering tactics, and implement strong controls to limit chance one employee can fall victim
- Safeguard payee data, and segregate duties. Verify changes by going to the source on file.
- Utilize audit logs and user access to banking and system information





## Reminders & best practices (cont.)

### Credit card controls:

- Establish limits, require reconciliations by card holders, and require supervisors to review and hold card holders accountable
- Standardize the submission and review process. Clarify what proper support looks like
- Review and update the number of cards, cardholders, and limits at least annually
- Train cardholders and require certification



## Credit card controls (cont.)

### Before issuing cards...

- Ensure cardholders have business need (Oprah doesn't run the District)
- Establish card limits based on spending expectations (limits loss)
- Require cardholder agreements
- Segregate the process to order and issue cards






## Credit card controls (cont.)

### Enforce a good secondary review

- Creates accountability for cardholders
- Consider a reviewer/supervisor checklist
- Create standard forms for reviews
- Establish a workable deadline, ensure these are manageable by the employee based on schedule or other limitations



# Disbursement resources




## Accounts Payable Guide

**Improving your processes:**  
Tips for leaders, managers, supervisors and accounts payable clerks

Center for Government Innovation

Brought to you by the Center for Government Innovation, a service of the Washington State Auditor's Office

First edition, November 2021



Center for Government Innovation

### Internal Control Checklist for Payroll Processes

Date of Review: \_\_\_\_\_  
Reviewed by: \_\_\_\_\_  
Key recommendations: \_\_\_\_\_

Instructions: Answer questions below as they relate to the payroll function. Further evaluate any "no" answers to determine if there are compensating controls in place, or if recommendations should be made to improve internal controls. Some questions include additional clarification in cell comments.

Category	Question (see cell comments in some cases for more clarification)	Yes	No	N/A	Comments
Resource records	1. Are personnel files maintained for all employees, independent of department or position, in a secure location?				
	2. Are personnel records and supporting records (e.g., health, insurance, benefits) protected and accessible only to authorized personnel?				
	3. Do personnel files include records of appointment, salary, transfers, promotions, demotions, and other personnel actions and disciplinary actions?				
	4. Does the payroll clerk maintain a schedule, or other record, of the payroll process to ensure the payroll is processed on time?				
	5. Are all suggestions submitted by a department official and the documentation retained? Are records, when reviewed, used to correct the payroll process?				
Timekeeping	6. Are all employees paid for the time they actually work, but management approved to be paid for, and the time card is checked for accuracy and approved by the employee?				
	7. Are employees paid for the time they actually work, but management approved to be paid for, and the time card is checked for accuracy and approved by the employee?				
	8. Are the time and attendance records approved by a supervisor or manager before being used for payroll?				
	9. Do managers use time cards to track their own time, and are they approved by a supervisor or manager before being used for payroll?				
	10. Are time cards checked for accuracy and approved by the employee and the supervisor before being used for payroll?				
	11. Are payroll records reviewed by a supervisor or manager before being used for payroll?				
	12. Are payroll records reviewed by a supervisor or manager before being used for payroll?				
	13. Are payroll records reviewed by a supervisor or manager before being used for payroll?				
	14. Are payroll records reviewed by a supervisor or manager before being used for payroll?				
	15. Are payroll records reviewed by a supervisor or manager before being used for payroll?				
	16. Are payroll records reviewed by a supervisor or manager before being used for payroll?				
Time diary (if applicable)	17. Is the time diary used when a supervisor approves?				
	18. Is the time diary used when a supervisor approves?				
Payroll process	19. Are payroll checks prepared and signed by the payroll clerk, and are they reviewed by a supervisor or manager before being issued?				

Center for Government Innovation

## Best practices for travel and reimbursable expenses



Office of the Washington State Auditor  
Pat McCarthy

January 2024

Best practices for travel and reimbursable expenses | 1

Center for Government Innovation

## Best practices for credit card programs



Office of the Washington State Auditor  
Pat McCarthy

July 2019

Best practices for credit card programs | 1

Credit card programs vary in their nature and size, as well as how the credit cards are used – all of which affect risk of unallowable purchases.

Programs can include traditional credit cards (such as Visa or Mastercard), procurement cards, or merchant cards that allow purchases at a specific retail establishment.

Credit cards can make it easier and less costly to make certain purchases, but there is also an increased risk for misuse or mismanagement. This risk needs to be planned for and mitigated.

The following are some best practices governments might consider when evaluating a credit card program and the related internal controls:





## Small and attractive assets

## Reminders and best practices

- Understand requirements: perform risk assessment, implement measures to track and control, consider cost/benefit in risk analysis
- Reminder: federal purchases must comply with 2 CFR 200.313.
- Set dollar thresholds by class, not one-size fits all
- Be consistent between departments
- Maintain central control over the asset listing, or at the least central oversight





## Steps to an asset risk assessment

- Identify noncapital assets, by type
- For each type, identify risks by answering:
  - Is this a new type?
  - What does the public expect?
  - Is this risky?
  - Could this be used for personal use?
  - Could this go missing easily?
  - Is it dangerous?
  - etc.
- For each risk, identify likelihood
- Develop proper safeguards
- Review risks again, and monitor for effectiveness





## Assets: Take-home vehicles

# Best practices to manage your fleet

## Getting started:

- A robust policy starts with the basics: employee qualifications, expectations, process to assign and limit use

## Assigning vehicles:

- Consider your eligibility criteria, confirm with actual data, and centralize the review/approval process





## Assets: Take-home vehicles (cont.)

## Best practices to manage your fleet

Set smart thresholds and use your data:

- Establish proper minimums, and impose mileage limits
- Review short-term authorizations
- Keep track of assignments and records
- Mileage logs will help inform decisions and reinforce policies



# Scan to access the Resource Library



**Best practices for take-home vehicle programs**

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

Some governments allow select employees to drive their assigned work vehicle home, otherwise known as a take-home vehicle. Governments can justify this practice because it benefits them or the public in some substantial way. For example, an employee may frequently respond to after-hour emergencies occurring away from their normal duty station using specialty equipment. By having access to a take-home vehicle, that employee can respond faster to the emergency location.

January 2025

**Best practices for credit card programs**

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

Government credit card programs vary greatly in size and purpose, as they allow employees to pay for travel, fuel or small

**Best practices for tracking small and attractive assets**

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

Governments own a variety of assets that fall below their capitalization threshold for financial reporting purposes that require safeguarding. We call them small and attractive assets here

**Best Practices for Sending Wire Transfers**

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

Wire transfers move money from one bank account to another almost instantaneously. They are generally considered safe as long as the sender is confident the transaction is valid, and the wiring instructions are accurate. In today's environment, those can be hefty assumptions.

Wire transfers are typically used to transfer larger sums of money, and usually only for limited purposes due to the higher transactional cost. For example, governments might use them to make investment purchases, debt payments, or potentially to purchase property.

**ESSENTIALS OF MANAGING FEDERAL AWARDS**

A COMPLIANCE HANDBOOK

Center for Government Innovation

**Best Practices for ACH Electronic Payments**

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

Governments are increasingly using Automated Clearing House (ACH) payments to pay employees and vendors, replacing more costly checks and warrants. These are electronic bank-to-bank payments processed in batches through the ACH Network. They have their own unique risks that are different from checks and warrants, and these risks are too large to ignore.

Today, bad actors target ACH transactions using social engineering or by having direct system access. In social engineering schemes, bad actors may pose as vendors to get employees to approve changes to contact and/or bank account information in order to divert payments. Employees and others with system access can also perpetrate fraud, such as by adding fictitious vendors or changing a vendor's bank account information to their own or that of an accomplice.



# Questions?

**Niles Kostick, Manager**  
Center for Government Innovation  
Center@sao.wa.gov  
(564) 999-0816



Office of the Washington State Auditor