

# Achieving Objectives and Preventing Fraud

---

... is easier than you think.



December 5, 2024

Clark County Audit Services

# Today

---

8:30 Opening remarks by County Auditor Greg Kimsey

8:35 It's All About the Risk

9:30 Break

9:40 To Catch a Fraudster

10:35 Washington State Auditor's Office Government  
Innovation Center

11:20 Closing remarks by Mark Gassaway



# It's All About the Risk

---

## Why Internal Controls Rule Our Lives

Larry Stafford

12/5/2024



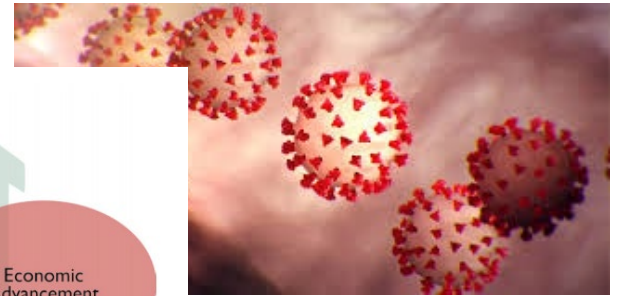
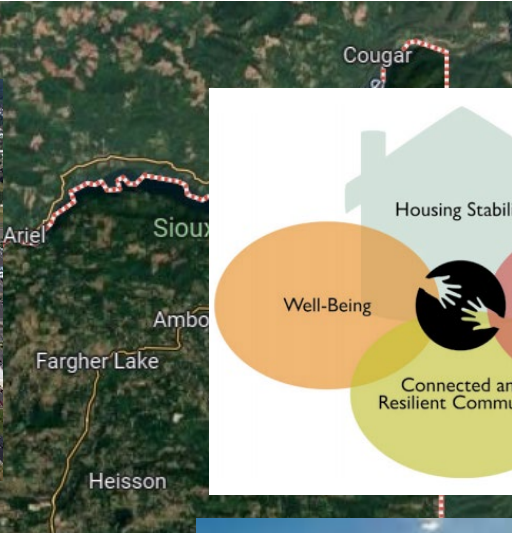
# RISK



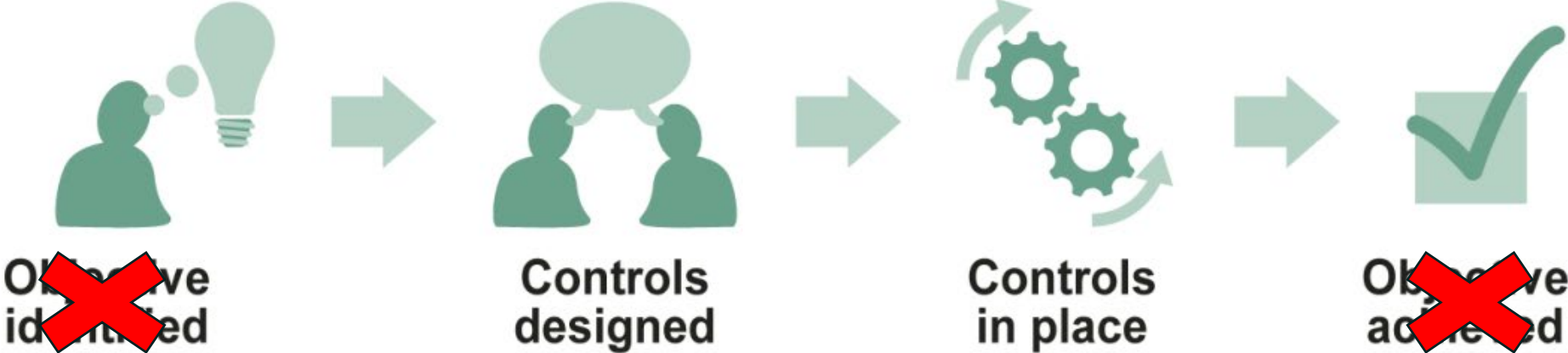
Employment Application			
<b>Standard Application for Employment</b>			
<small>If it is our policy to comply with an applicable state and federal law prohibiting discrimination in employment based on race, sex, color, sex, religion, national origin, disability or other protected characteristics, please carefully read and answer all questions. You will not be considered for employment if you fail to completely answer all the questions on this application. You may attach a resume, but all questions must be answered.</small>			
"Employee"		Position applying for	
<b>PERSONAL DATA</b>			
Name (last, first, middle)			
Street address (not mailing address)		City	State Zip
Home telephone number	Business telephone number	E-mail address	
Are you over 18 years old?	Are you a U.S. citizen?	Do you have a valid driver's license?	



# RISK



# REDUCE RISK WITH CONTROLS



**RISKS TO  
OBJECTIVES  
IDENTIFIED!**



**INCREASE  
CERTAINTY OF  
ACHIEVING  
OBJECTIVE**



# Goals

---

Increase our ability to:

1. Identify risk
2. Evaluate risk
3. Manage risk



# Identifying Risk Using Uncertainty

---



**Likelihood**



**Impact**



# Evaluating Risk: Simple, Complicated, or Complex

---

## Simple

- Issues that are known by your profession and often have solutions or best practices
- Example: Changing to a different operating standard
- Approach: Follow industry / best practice

## Complicated

- Issues that can be separated in logical way based on rules, laws, etc. but may have “known unknowns”
- Example: Implementing a new regulatory requirement for reporting data
- Approach: chunk down and evaluate each component



# Evaluating Risk: Simple, Complicated, or Complex

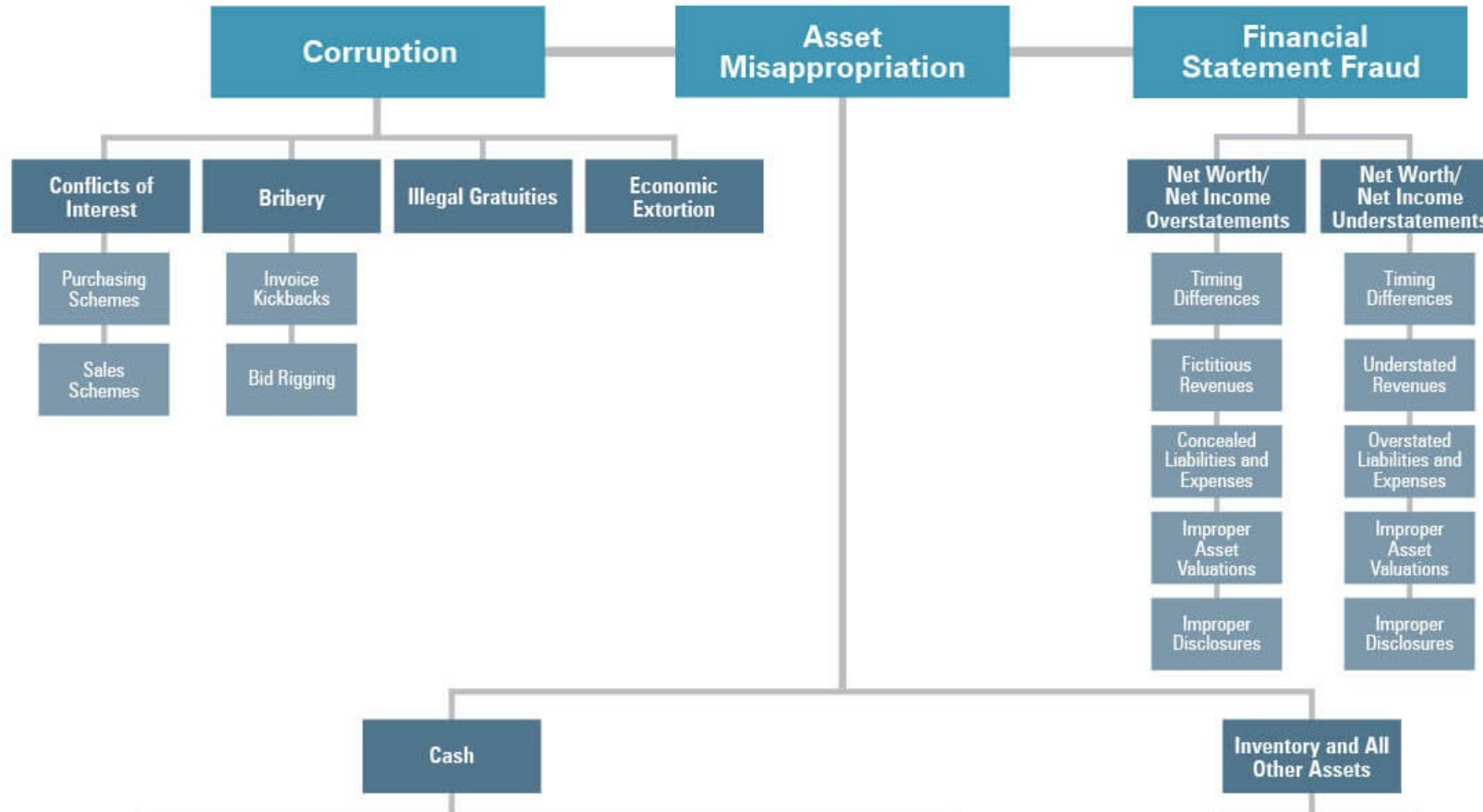
---

## Complex

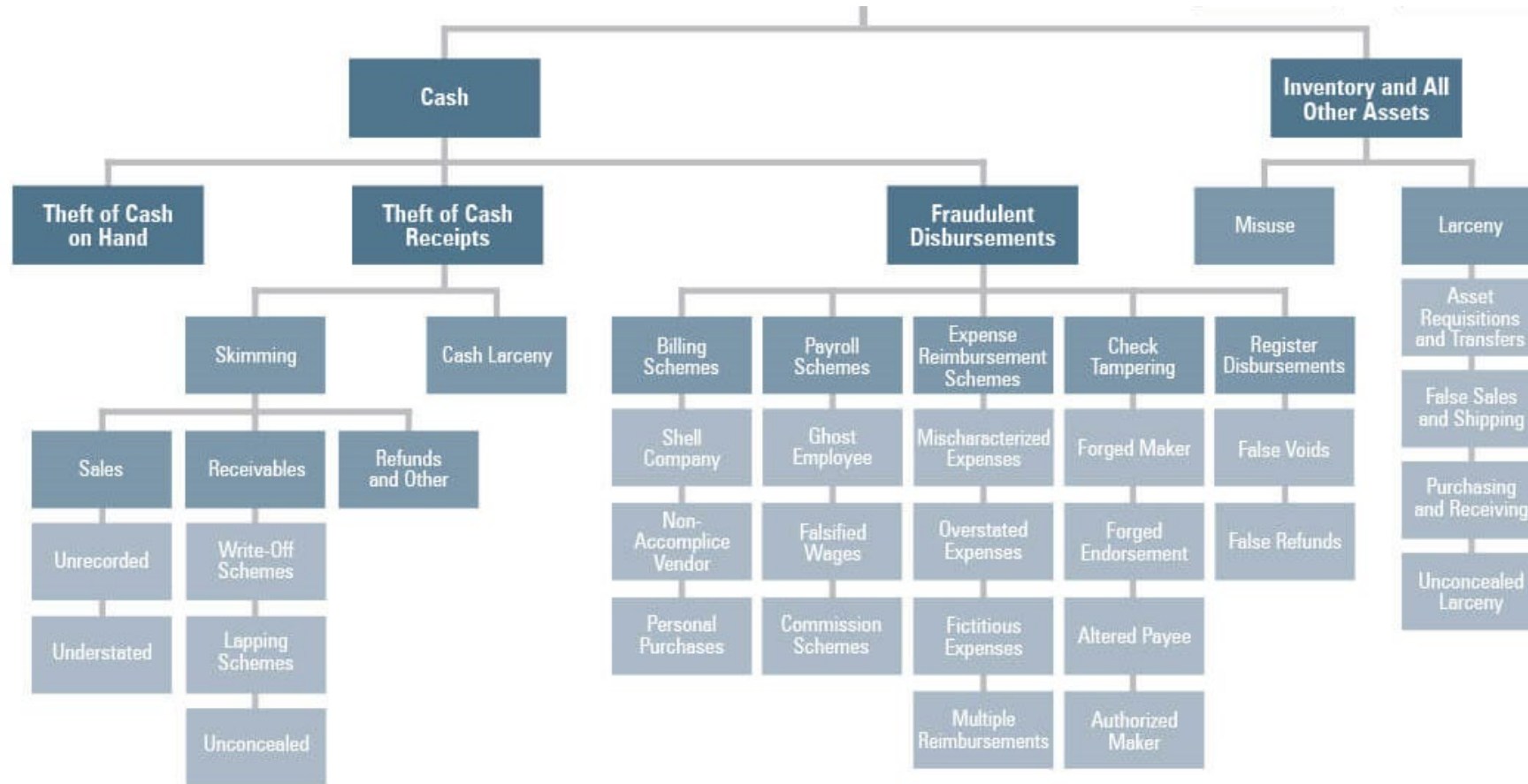
- Issues with little or no order or predictability and have “unknown unknowns”
- Example: Work that is weather dependent
- Approach: Iterative and ongoing evaluation process



# Evaluating Risk: Fraud Tree



# Evaluating Risk: Fraud Tree

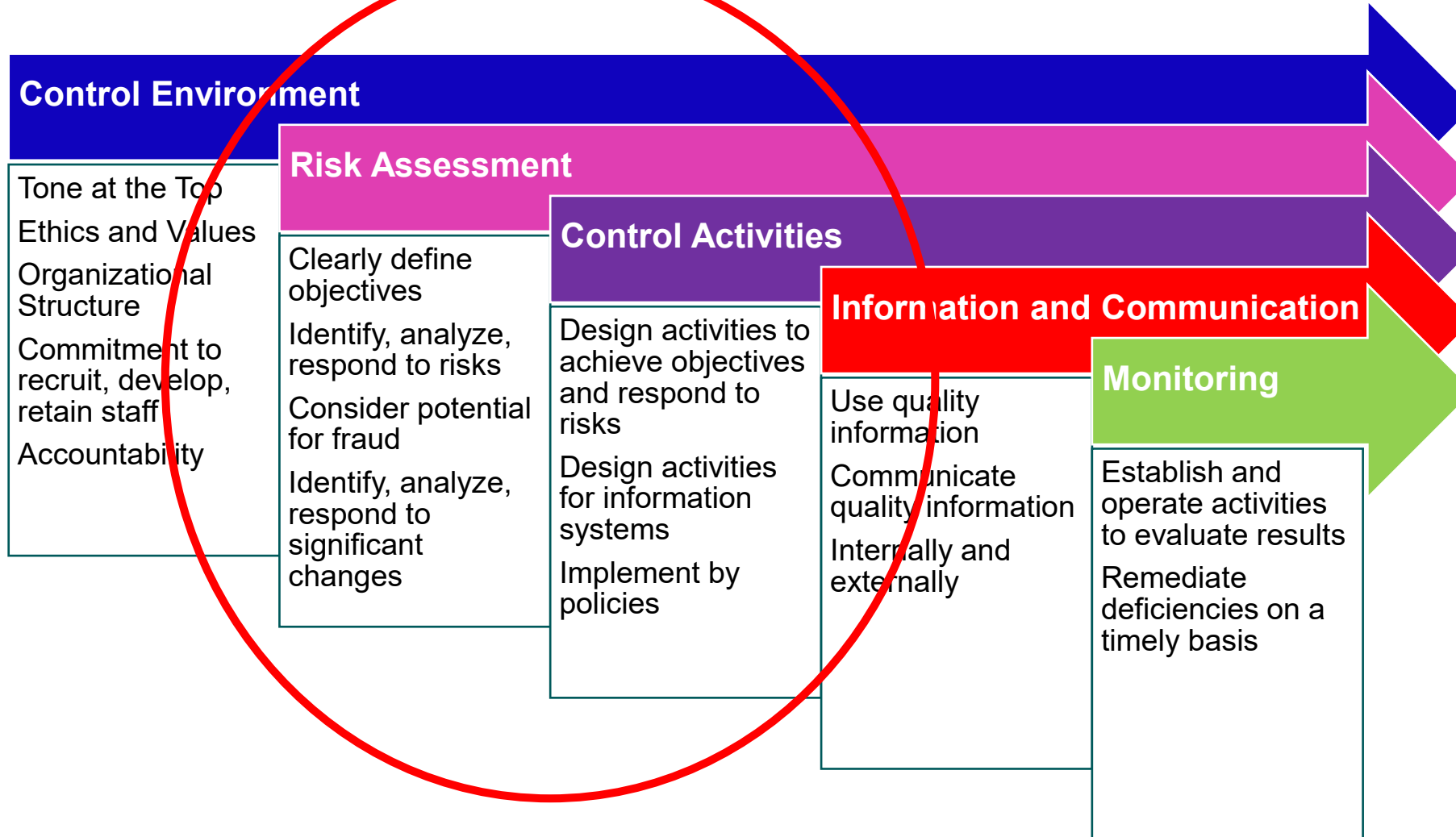


# Evaluating Risk: Fraud Triangle

---



# Managing Risk: System of Internal Controls



# Summary

---

- **Risk = uncertainty of outcomes of actions or decisions**
  - Objectives: Operating, Reporting, Compliance
- **Evaluating Risk**
  - Likelihood and Impact
  - Simple, Complicated, or Complex
  - Fraud Tree and Triangle
- **Manage Risk with a system of controls**



# Resources

---

[Standards for Internal Control in the Federal Government | U.S. GAO](#)

[Association of Certified Fraud Examiners: Fraud 101: What is Fraud?](#)

- Fraud Tree and Fraud Triangle
- Categories of Fraud





*“The only thing necessary for fraud to happen is for good people to do nothing.”*

–Me



# Thank you!

## Comments and questions

**GREG KIMSEY, CLARK COUNTY AUDITOR**

**AUDIT SERVICES**

**Larry Stafford, Audit Services Manager**

**Arnold Pérez**

**Michael Nash**

1300 Franklin Street Suite 575, P.O. Box 5000, Vancouver, WA 98666-5000

*For further information about this contact: Clark County [Audit Services](#)  
Via email [AuditServices@clark.wa.gov](mailto:AuditServices@clark.wa.gov) or phone (564) 397-2310 ext.4795*

###

*For other formats, contact the [Clark County ADA Office](#): **Voice** (564) 397-2322  
**Relay** 711 or (800) 833-6388; **Fax** (360) 397-6165; **E-mail** [ada@clark.wa.gov](mailto:ada@clark.wa.gov)*



# To Catch a Fraudster

---

Fraud Examples and Lessons from Other Governments in Washington

Michael Nash

December 5, 2024



# Today's Agenda

---

- Revisit Risk and Internal Control
- ***How is fraud detected?*** The lines of defense model
- Example Fraud Cases
  - How was the fraudster caught?
  - Discussion: could / should it have been caught sooner?
  - Insights from 2024 Annual Report from Association of Certified Fraud Examiners (ACFE)



# Risk and Internal Control

**Risks.** They exist, we have 'em.

We develop *systems of internal control* to address that **Risk**.

An effective *system of internal control* has 5 components

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

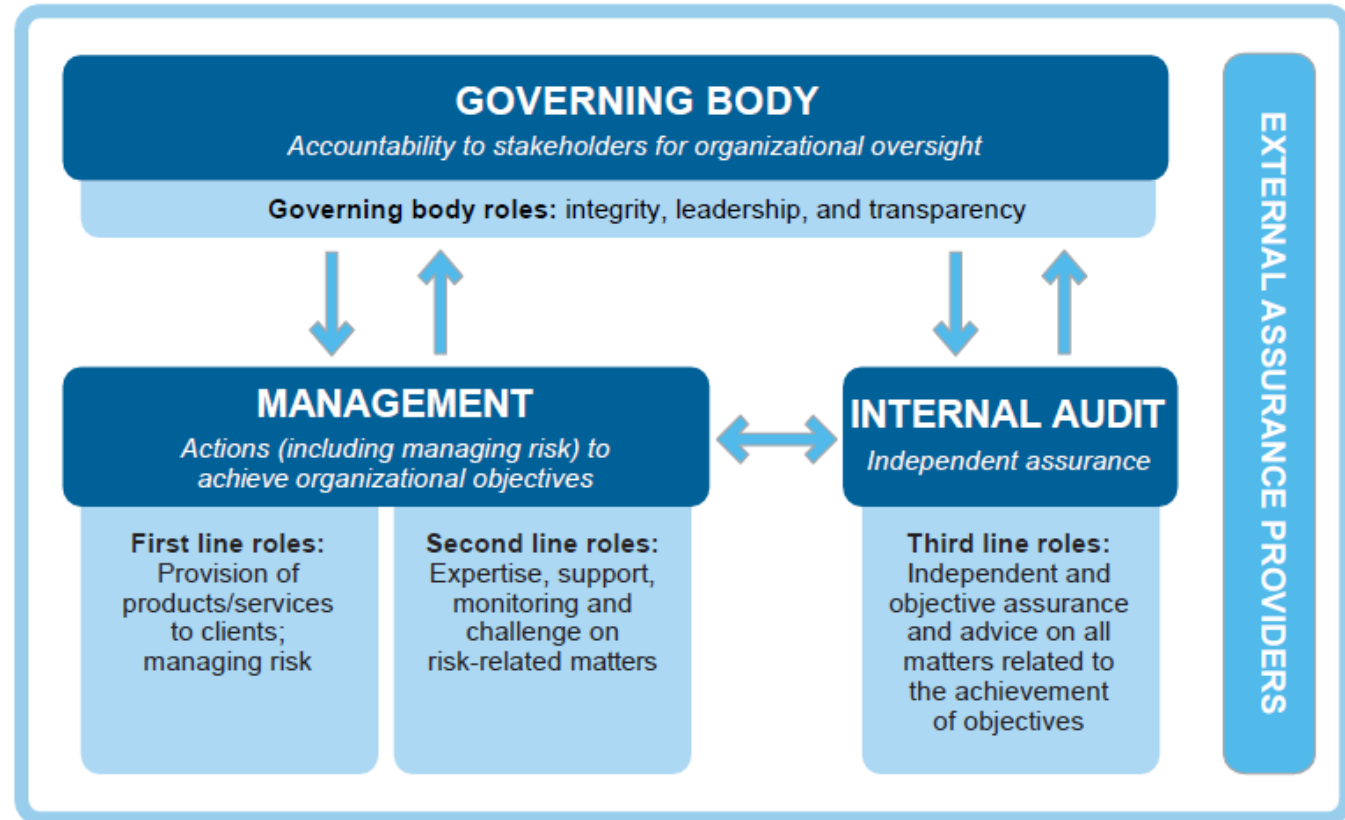


# The Three Lines of Defense Model

Who's **responsible** for the system of internal controls?

How is that **responsibility** divided?

## The IIA's Three Lines Model



# How is Fraud Detected?

## First line of Defense:

- Control activities

## Second line:

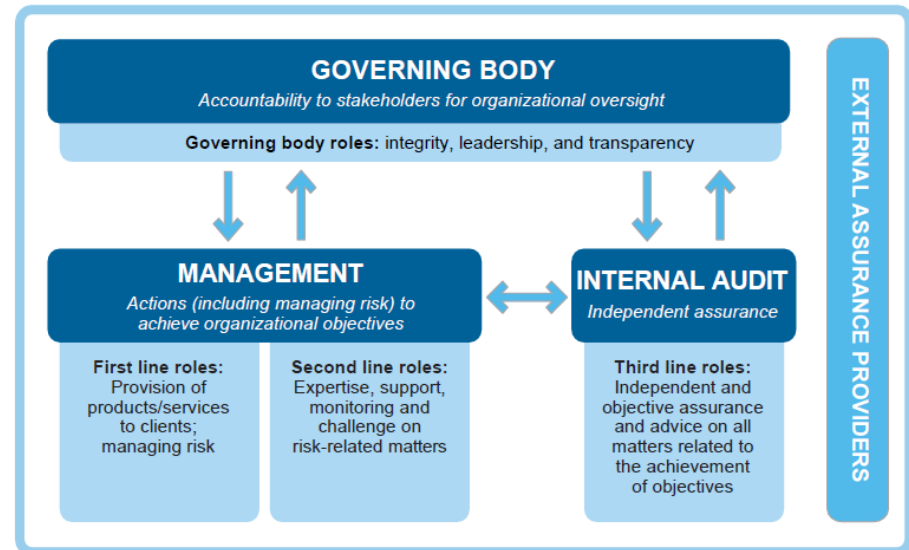
- Information and communication, monitoring – **Professional Skepticism!**
- The design, implementation, and ongoing monitoring of internal controls are a management responsibility.

## Third line of defense

- Independent, objective assurance

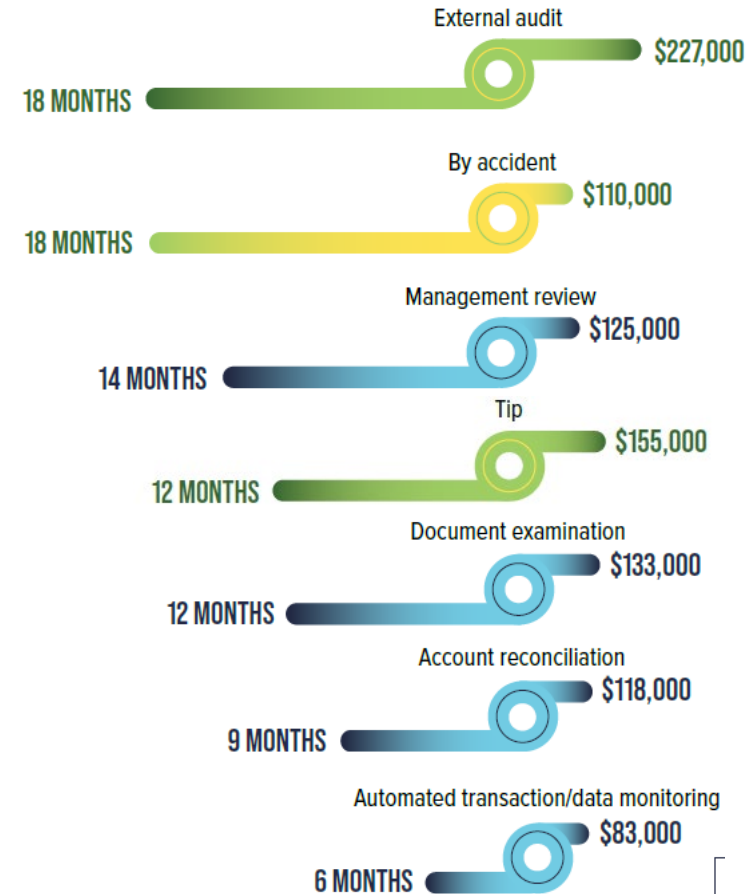
Other parties: whistleblowers, customers, concerned citizens, law enforcement

## The IIA's Three Lines Model



# The Cost of Late Defense

- The cost of fraud and the time to detect increases with each line of defense breached.
- Timelines for detection by parties outside of the lines of defense
- The value of preventative controls





# How was the fraud detected?

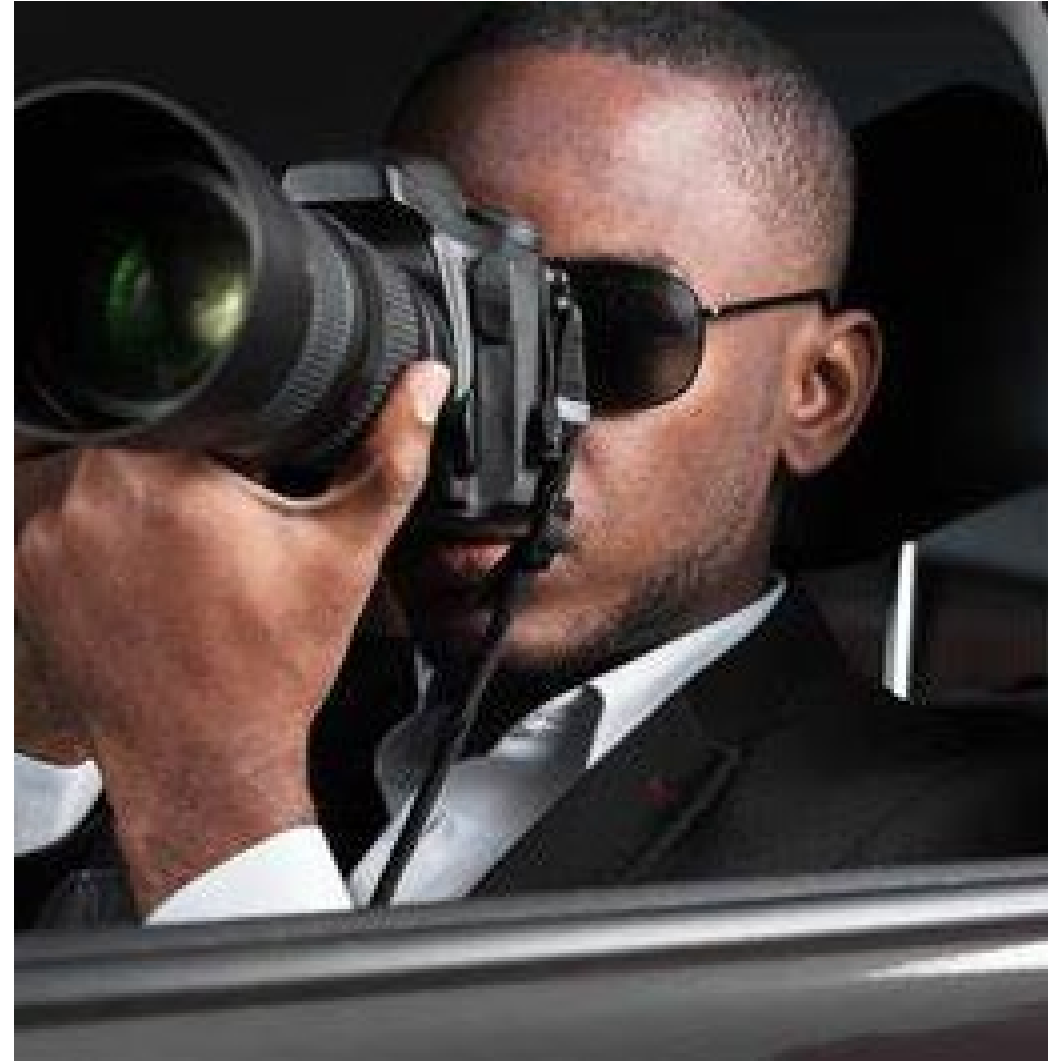
---

We're going to walk through several recent fraud cases from here in Washington.

After presenting each case, I'll ask you to vote in a poll on how the fraud was detected

1. First line of Defense: control activities
2. Second line: information and communication, monitoring – Professional Skepticism!
3. Third line of defense: audit (internal or external for this exercise)
4. Other parties: whistleblowers, customers, concerned citizens

**Clues:** timelines / amounts stolen, state of internal controls and segregation of duties, leadership “tone”



# Case #1: Pacific County

---

An investigation found that between April and December 2021, **\$9,659.36** of customer cash was misappropriated from deposits for the North District Court.

The misappropriated amounts were deposited back into the account between 4 and 124 days later.



# Case #1: Background

---

## Pacific County District Court

- Court Staff: Transact, balance and close out tills
- District Court Clerk: Prepares and deposits cash and checks daily. Performs the monthly bank reconciliations
- Court Administrator: Provides oversight / monitoring of multiple courts / clerks



# Case #1: How the Fraud / Loss Occurred

---

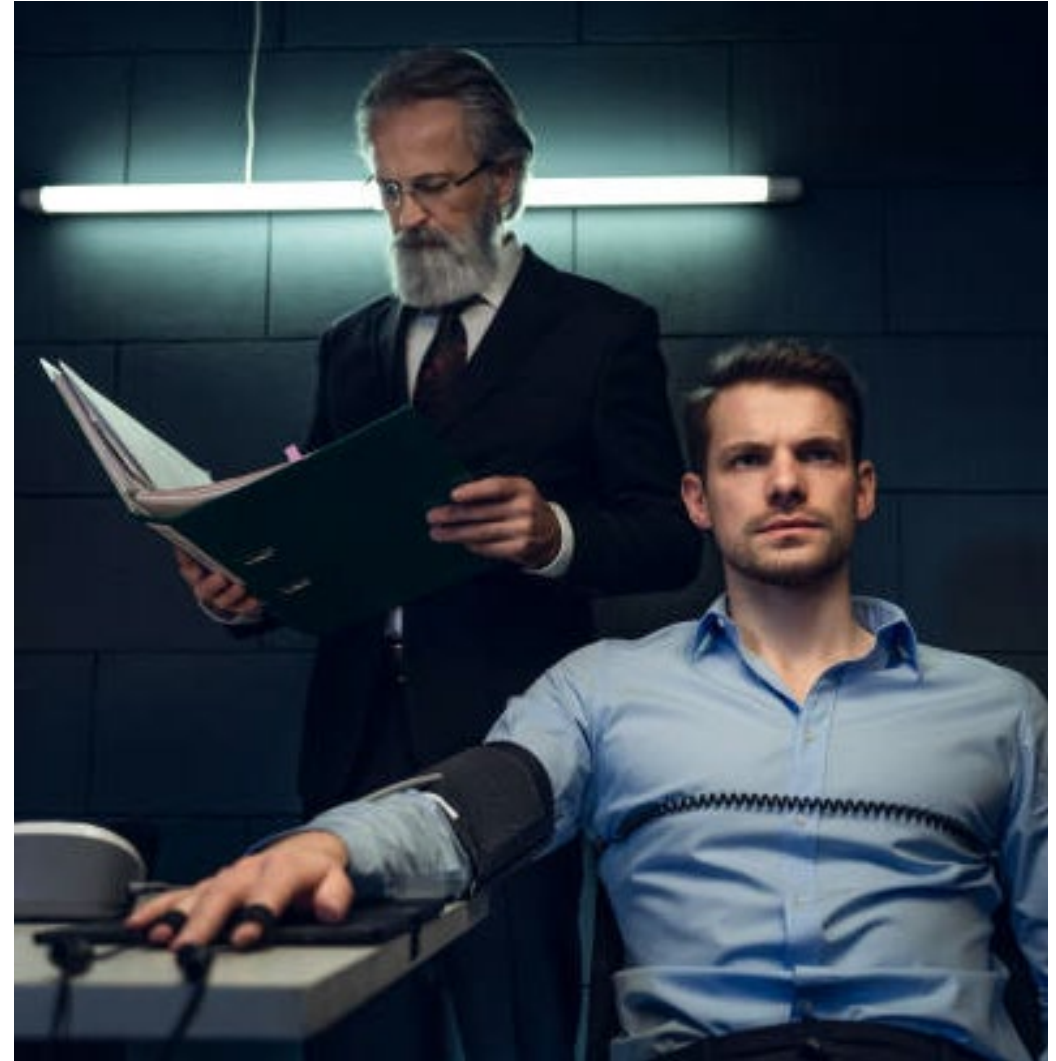
- On April 30, 2021 the North District Court took in \$1,833.93.
  - Money was not deposited until 33 days later
- Between August 18<sup>th</sup> and December 16<sup>th</sup>, 14 days worth of cash receipts were collected but not deposited timely.
  - Deposits for all 14 days were made on December 20<sup>th</sup> and 21<sup>st</sup>, 2021.
- The Clerk transferred employment to Public Works in May, 2022



# Poll #1: How was the fraud / loss detected?

---

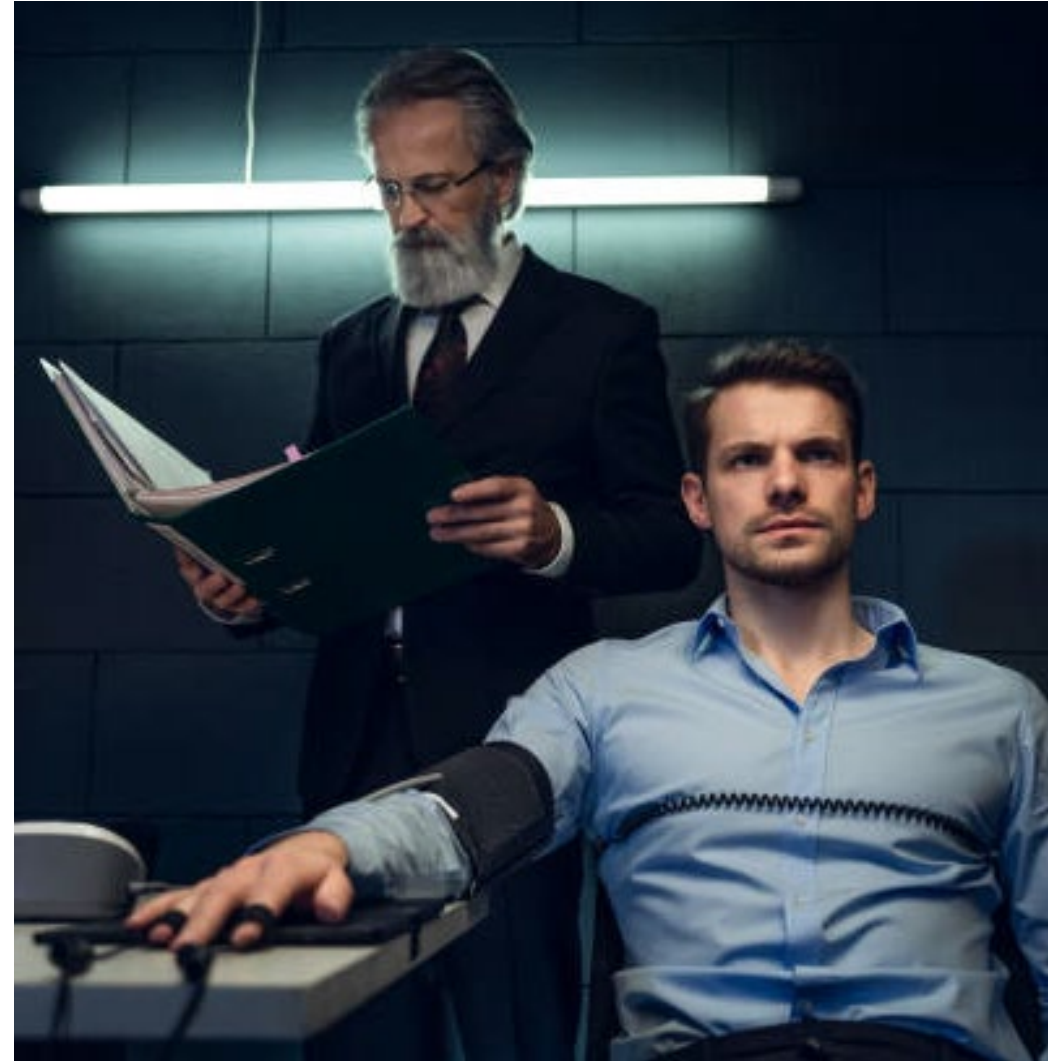
1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens



# Poll #1: How was the fraud / loss detected?

---

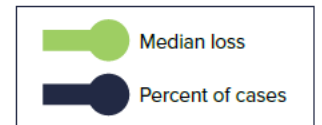
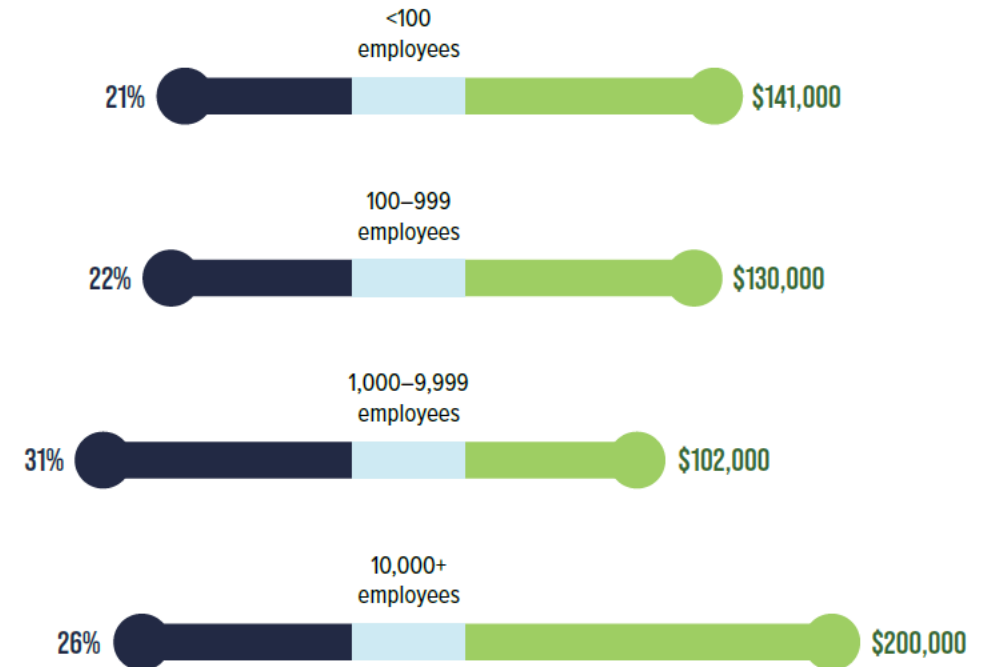
1. First line of Defense: control activities
2. **Second line: information and communication, monitoring**
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens



# Case #1: Discussion

## June 2022: Review / second reconciliation of 2021 bank deposits

- Noticed timing of some deposits
- Professional Skepticism



## Case #2: Yakima County Special Purpose Districts

---

An investigation found that between January 2019 and June 2023, a bookkeeper misappropriated \$9,151 in aggregate from seven special purpose districts in Yakima, WA.

Additionally, \$17,706 in questionable costs was identified.





# Case #2: Background

- Special purpose districts provide drainage / irrigation services.
  - Annual Revenues for the district range from **\$5,571** to **\$824,912**
  - Two of the districts have dedicated staff (4 FTE and 3 FTE). The rest of the districts have a small Board of directors / supervisors and no employees / staff.
- Bookkeeper: Employee of one district (Union Gap Irrigation) and was considered a contractor for the other districts.
- Most of the 7 districts did not have formal documentation of a contract in place for these services.



# Case #2: Background

---

- The Bookkeeper was responsible for:
  - Preparing budgets and financial reports for board approval
  - Processing district vendor payments, including costs for her own bookkeeping services and job-related expenses for which she requested reimbursement.
    - Some districts also delegated authority to submit expenses for reimbursement without prior approval
  - For Union Gap Irrigation District, the Bookkeeper was also responsible for preparing payroll, including her own pay disbursements. .



# Case #2: How the Fraud / Loss Occurred

- Between October 2019 and April 2023, the Bookkeeper used 26 invoices to submit 117 reimbursement requests for supplies.
  - Requested reimbursement from multiple districts for the full cost of the purchases.
- At Union Gap, she made several changes to payroll for herself and other employees (including a manager) to modify or remove withholdings.
  - She cashed out 50 hours of sick leave for \$1,563. However, policy did not allow sick leave cashouts.



# Case #2: How the Fraud / Loss Occurred

---

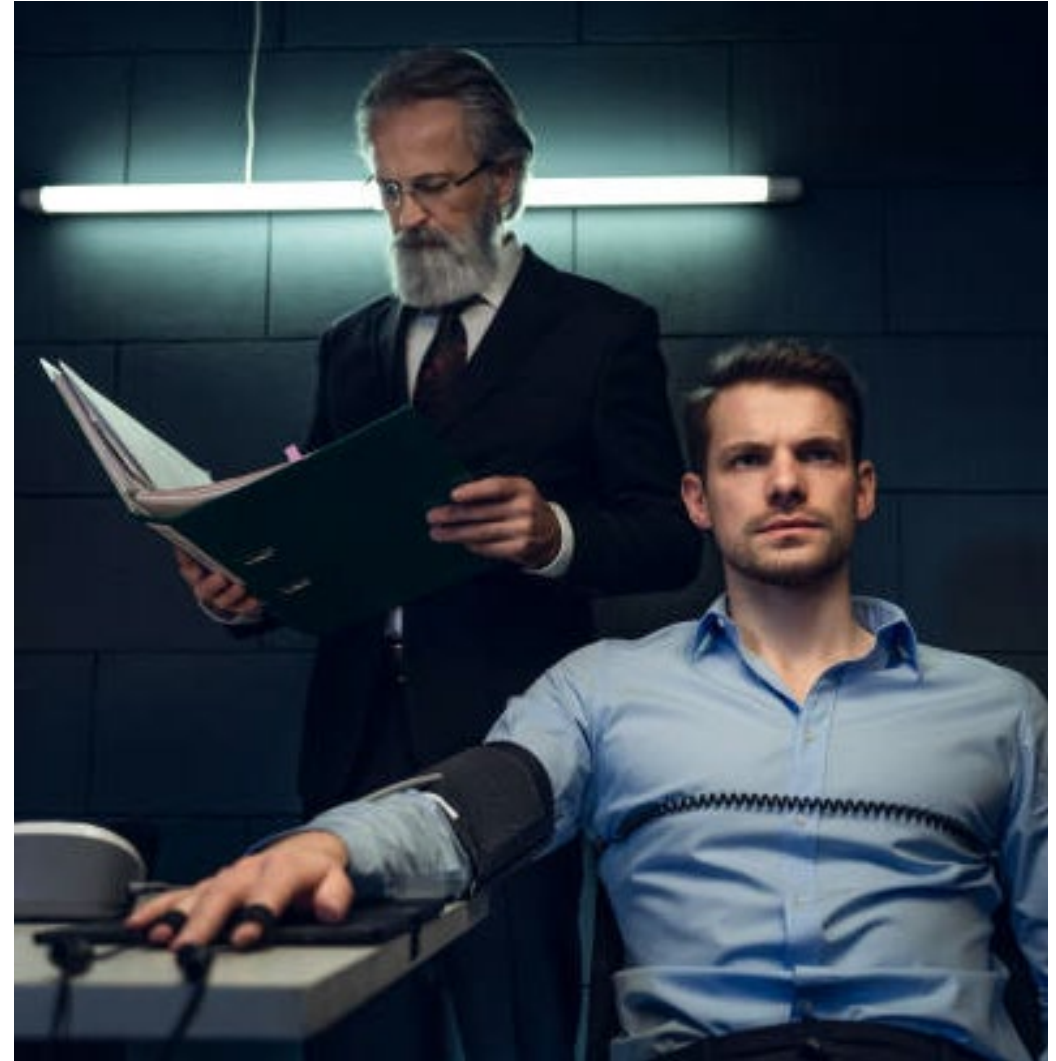
- Overbilled for services in excess of budgeted amounts
- Costs for bookkeeping services for District 12 exceeded budgeted amounts for the years 2020, 2021, and 2022 by \$8,664.
  - Total Revenue for District 12 in FY 2022 was \$5,571



# Poll #2: How was the fraud / loss detected?

---

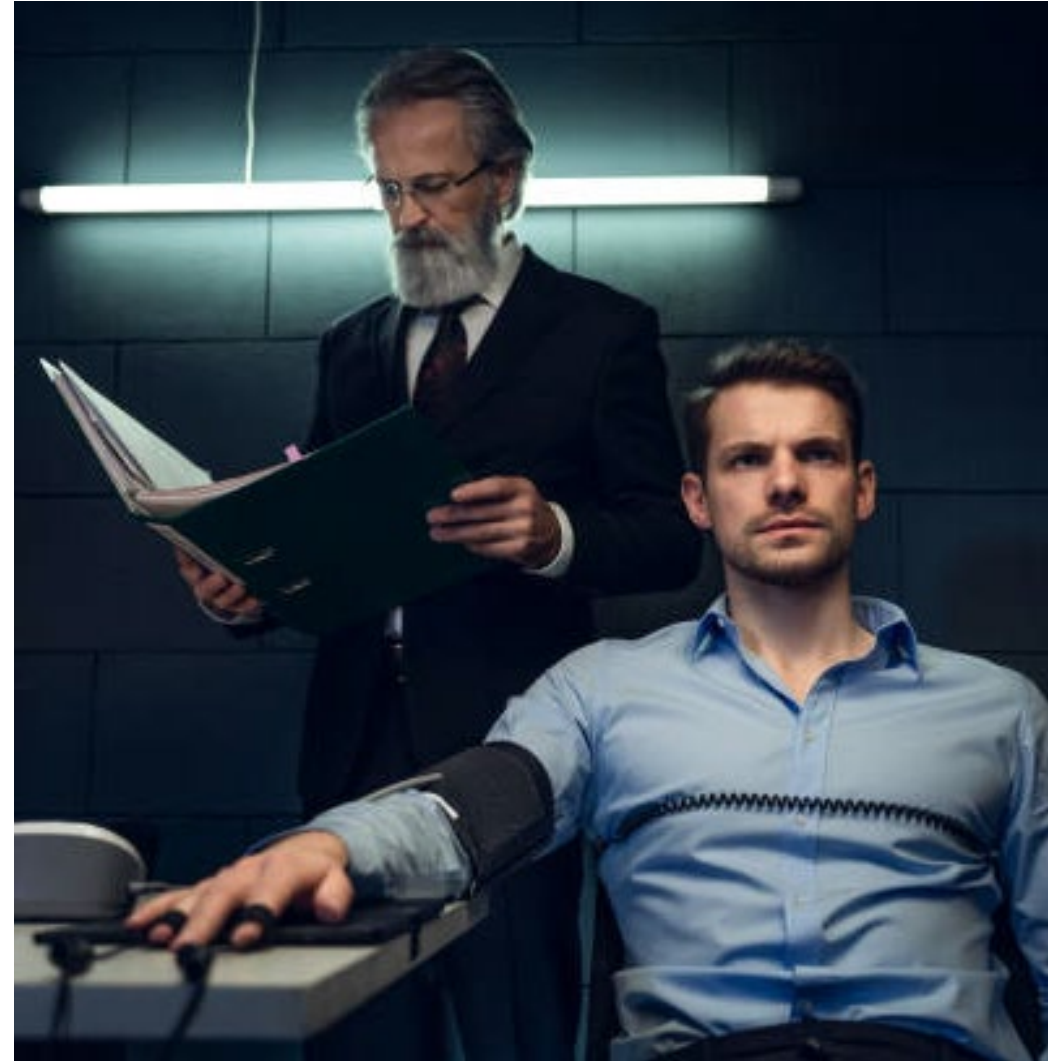
1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens



# Poll #2: How was the fraud / loss detected?

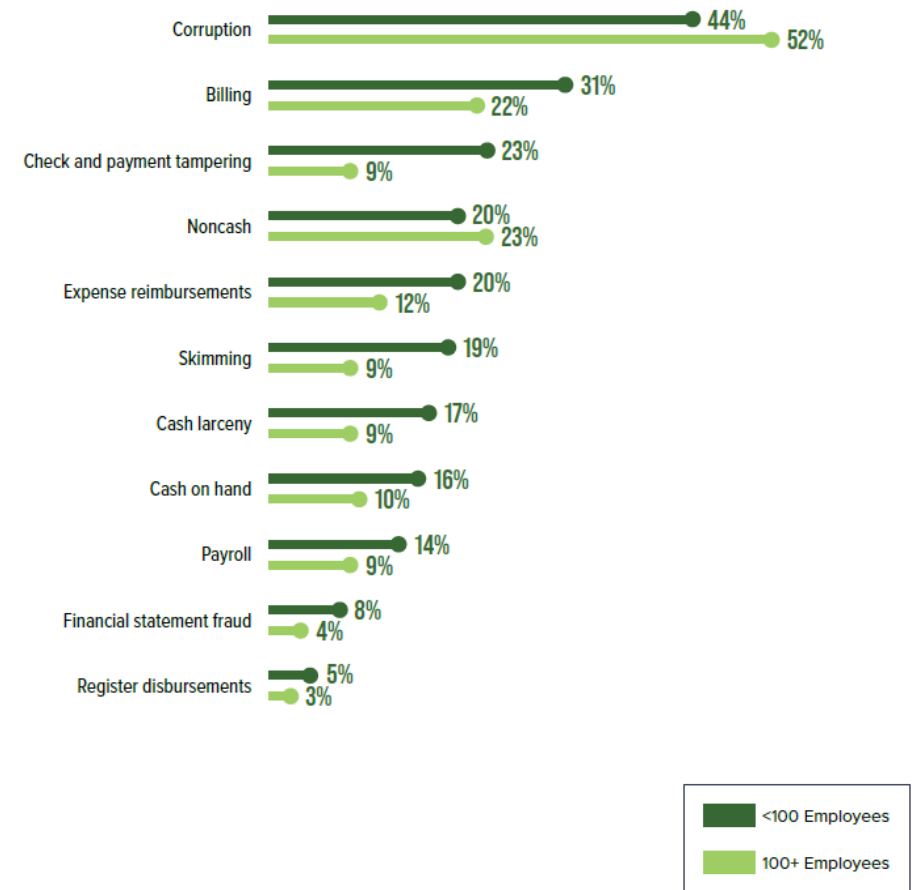
---

1. First line of Defense: control activities
2. **Second line: information and communication, monitoring**
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens



# Case #2: Discussion

- Board asked for bank statement
- Overbilling of supplies difficult to detect
- Small organizations / Functions lack staff resources to implement ideal controls



## Case #3: City of Morton

---

An investigation found that between February 4, 2013, and December 30, 2021 more than \$937,584 was misappropriated from the City of Morton

Morton: population just over 1,000 in Lewis County; budget of \$4.6 million; \$860,000 in annual tax revenue.





# Case #3: Background

- Morton has roughly 9 employees, including a fulltime Clerk-Treasurer and Deputy Clerk-Treasurer.
- The Clerk Treasurer oversees daily operations including handling bank deposits and reconciling the City's accounting system and bank statements.
  - Prepares checks (and can sign), records expenditures,
- Deputy: is primarily responsible for receipting City revenues and preparing weekly deposits for the Clerk-Treasurer to review and then deposit at the bank.



# Case #3: How the Fraud / Loss Occurred

---

- Deposit Theft Scheme: (\$311,727)
- The clerk treasurer failed to deposit customer cash payments into the City's bank account.
  - To conceal the theft, deposited vendor checks that she had received but not recorded in the accounting system.
  - Also wrote check from the City to the City to conceal the activity



# Case #3: How the Fraud / Loss Occurred

---

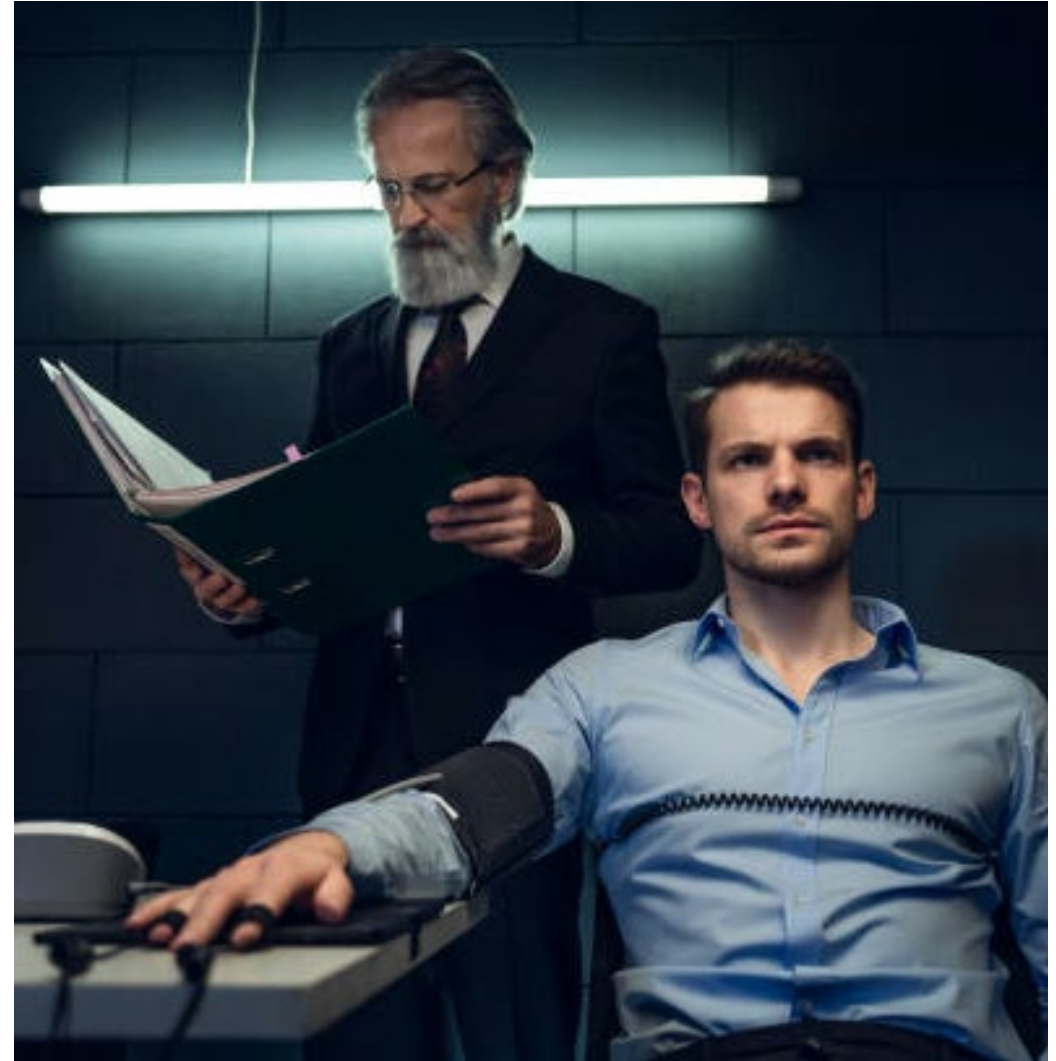
- Disbursements (\$625,857)
  - Between January 1, 2013 and March 31, 2022, and determined the Clerk-Treasurer wrote a significant number of City checks to herself
  - recorded them in the City's accounting system as payments to legitimate City vendors.
- \$10,000 of ATM cash withdrawals from the City's bank account between October 2019 and November 2021.
  - City officials could not find any records supporting the withdrawals.



# Poll #3: How was the fraud / loss detected?

---

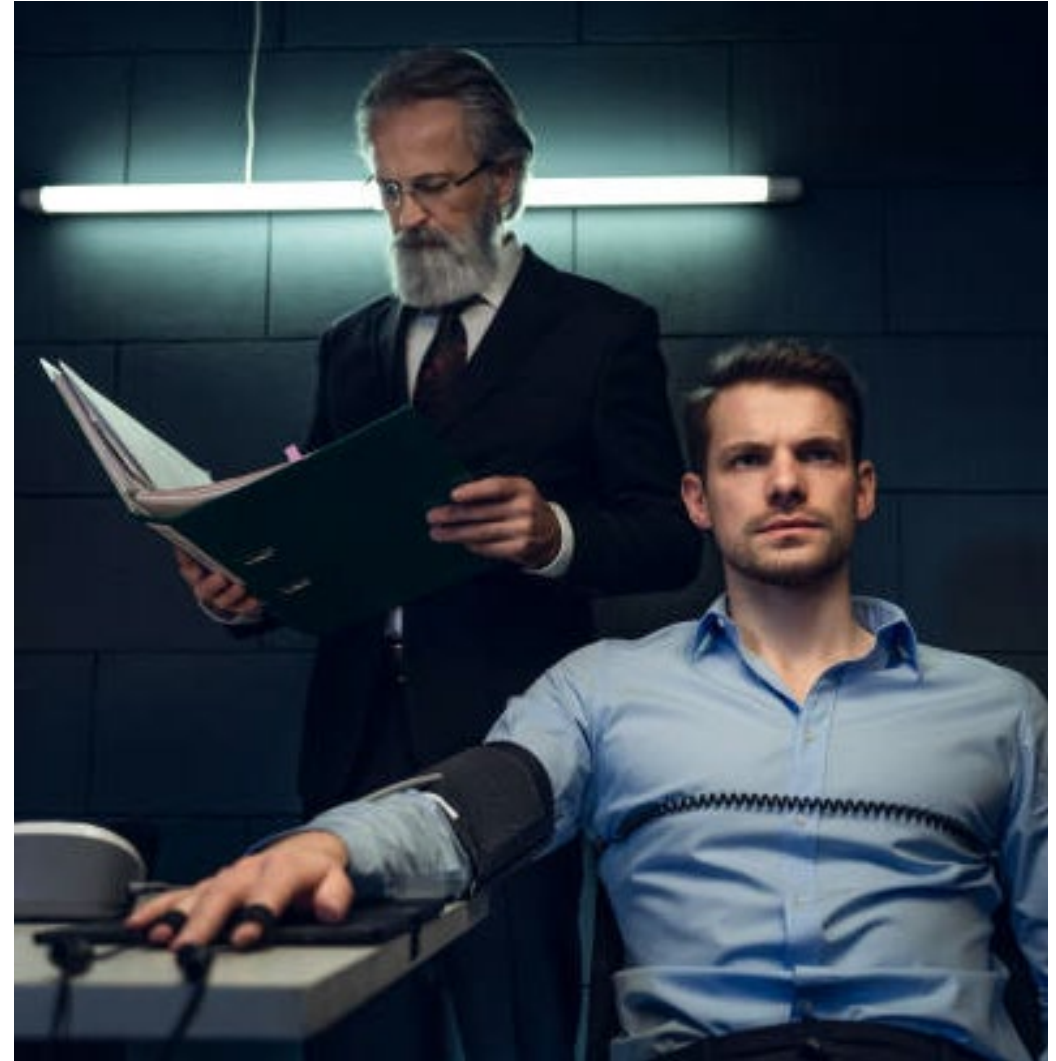
1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens



# Poll #3: How was the fraud / loss detected?

---

1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. **Third line of defense: Audit**
4. Other parties: whistleblowers, customers, concerned citizens



# Case #3: Discussion

- Auditors question why anyone was using p-cards for cash advances
- Two prior red flags identified by external audit went ignored
- Role of tone / organizational culture



# Case #4: Mason County Public Works

---

An investigation determined that **\$47,582** was misappropriated between April and September 2021.

Investigators were unable to assign responsibility for the loss.



# Case #4: Background

---

## Mason County Solid Waste Program

- Solid-waste landfill, transfer station, several smaller satellite stations
- 11 staff, with 1-2 staff at each receipting location
- **Attendants:** Closet out and balance tills, take to transfer station safe
- **Program Manager:** collects bags and takes them to public works departments
- **Accounting techs:** prepare deposit and makes deposit





# Case #4: How the Loss Occurred

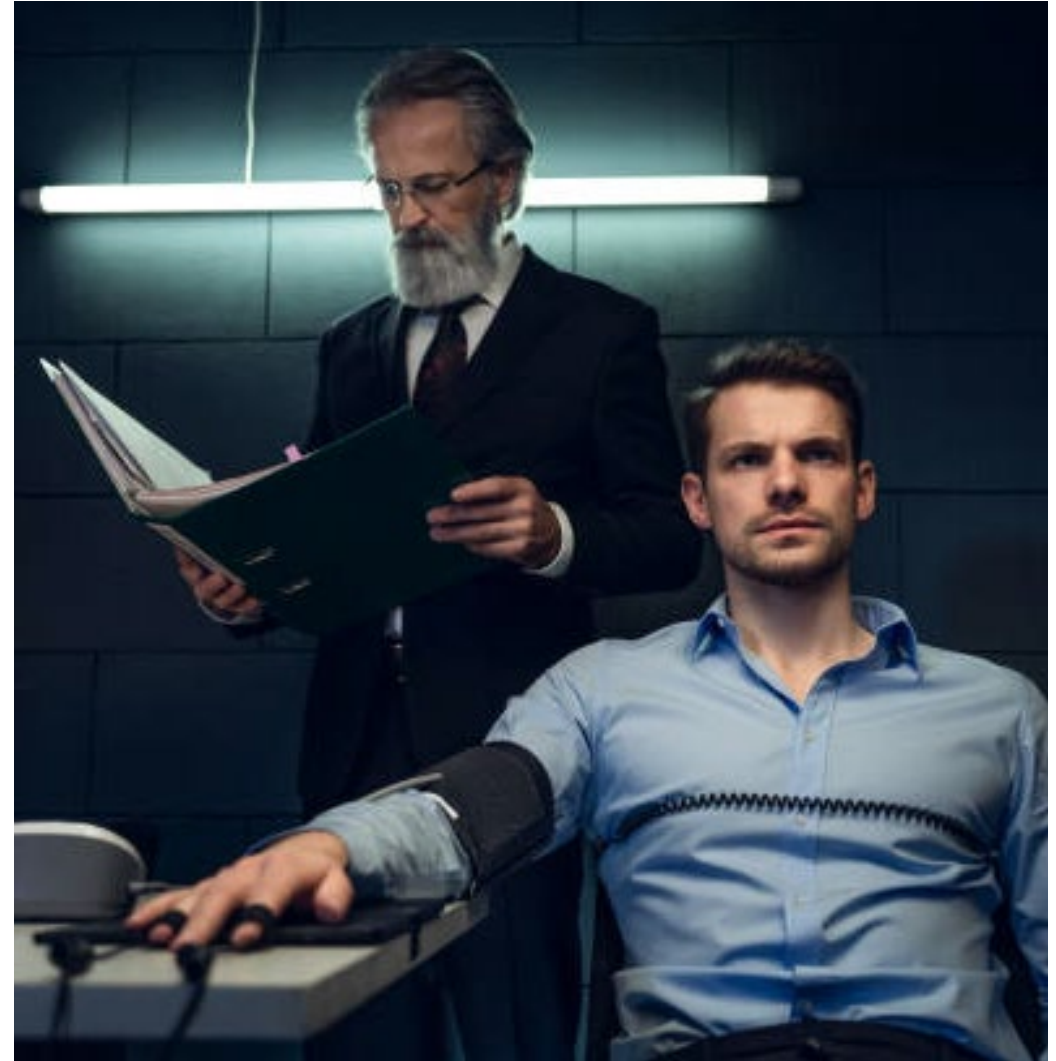
- Between April and September 2021:
  - 55 deposit bags went missing / were not deposited totaling \$47,582
  - Attendants: We just drop the bags in the safe
  - Program Manager: Picks up bags and transports. Does not count or document number of bags or check daily receipting reports.
  - Accounting Techs: Do not count number of bags or use / check daily receipting report
  - Access to safe at transfer station not controlled
  - Accounting techs area not secure and accessed by other staff regularly



# Poll #4: How was the fraud / loss detected?

---

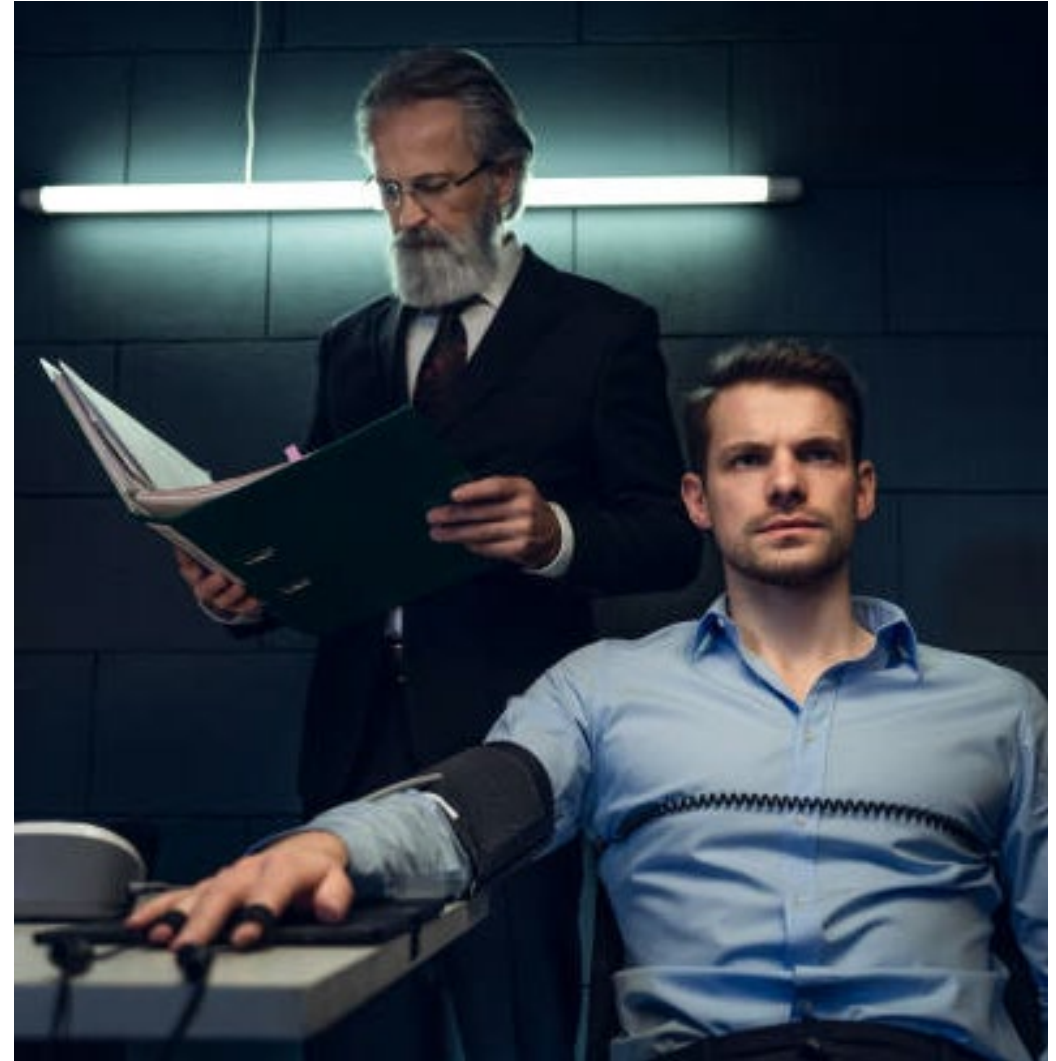
1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens



# Poll #4: How was the fraud / loss detected?

---

1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. Third line of defense: Audit
4. **Other parties: whistleblowers, customers, concerned citizens**



# Case #4: Discussion

- A customer called after noticing that their check payment had not cleared
- Internal control deficiencies
- Role of customers / vendors in controls?
- 43% of fraud detected by tip

FIG. 13 HOW IS OCCUPATIONAL FRAUD INITIALLY DETECTED?

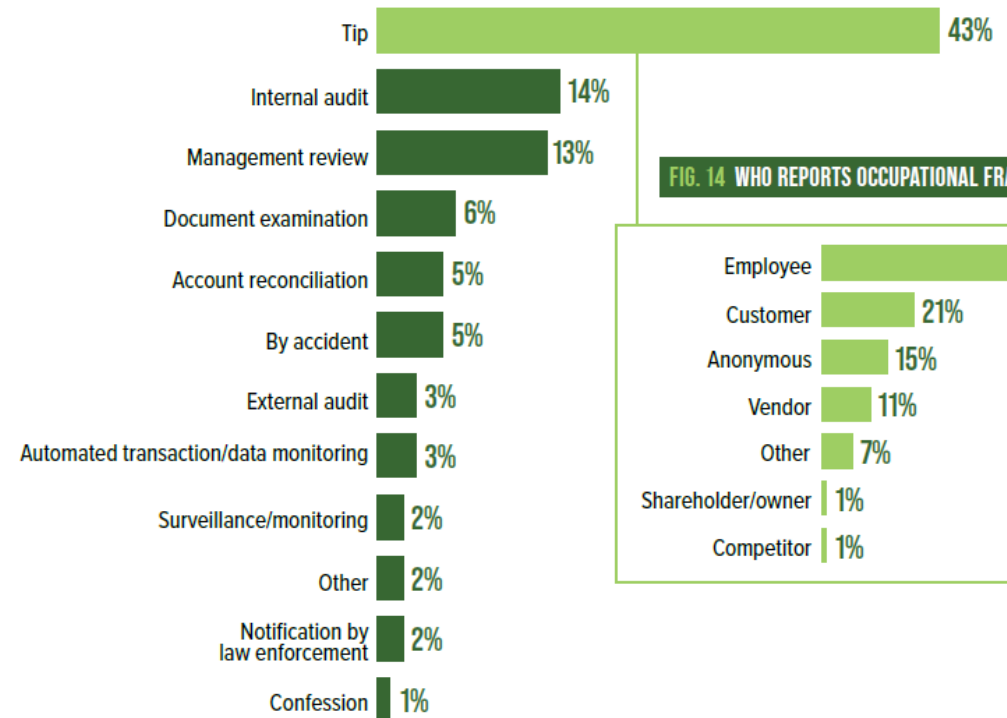
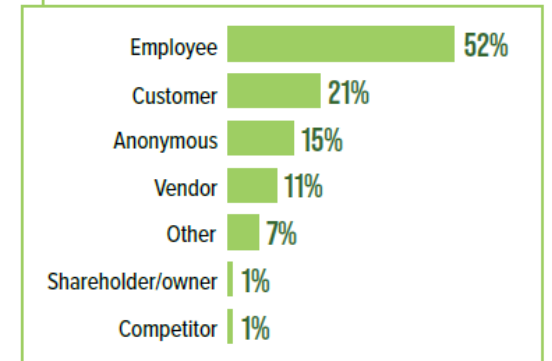


FIG. 14 WHO REPORTS OCCUPATIONAL FRAUD?



# Case #5: Office of Administrative Hearings

---

An Investigation determined that between June 2019 and May 2024, \$878,115 was misappropriated from Washington State Office of Administrative Hearings.

An additional \$4,933 in questionable costs was also identified.



# Case #5: Background

---

- The Office of Administrative Hearings conducts impartial administrative hearings for people and governments across the state.
- The Agency employs about 120 administrative law judges and 110 legal support and administrative staff
- In FY 2022:
  - \$31.9 million in total expenses
  - \$402,470 in credit card payments.



# Case #5: Background

- A chief administrative law judge directs the Agency's overall operations
- CFO: oversees the Agency's fiscal operations, including managing four fiscal department employees.
- Management analyst: served as the custodian of a credit card program.
  - oversaw card use
  - collected supporting receipts,
  - reconciled monthly statements
  - prepared payments to the credit card company



# Case #5: How the Fraud / Loss Occurred

---

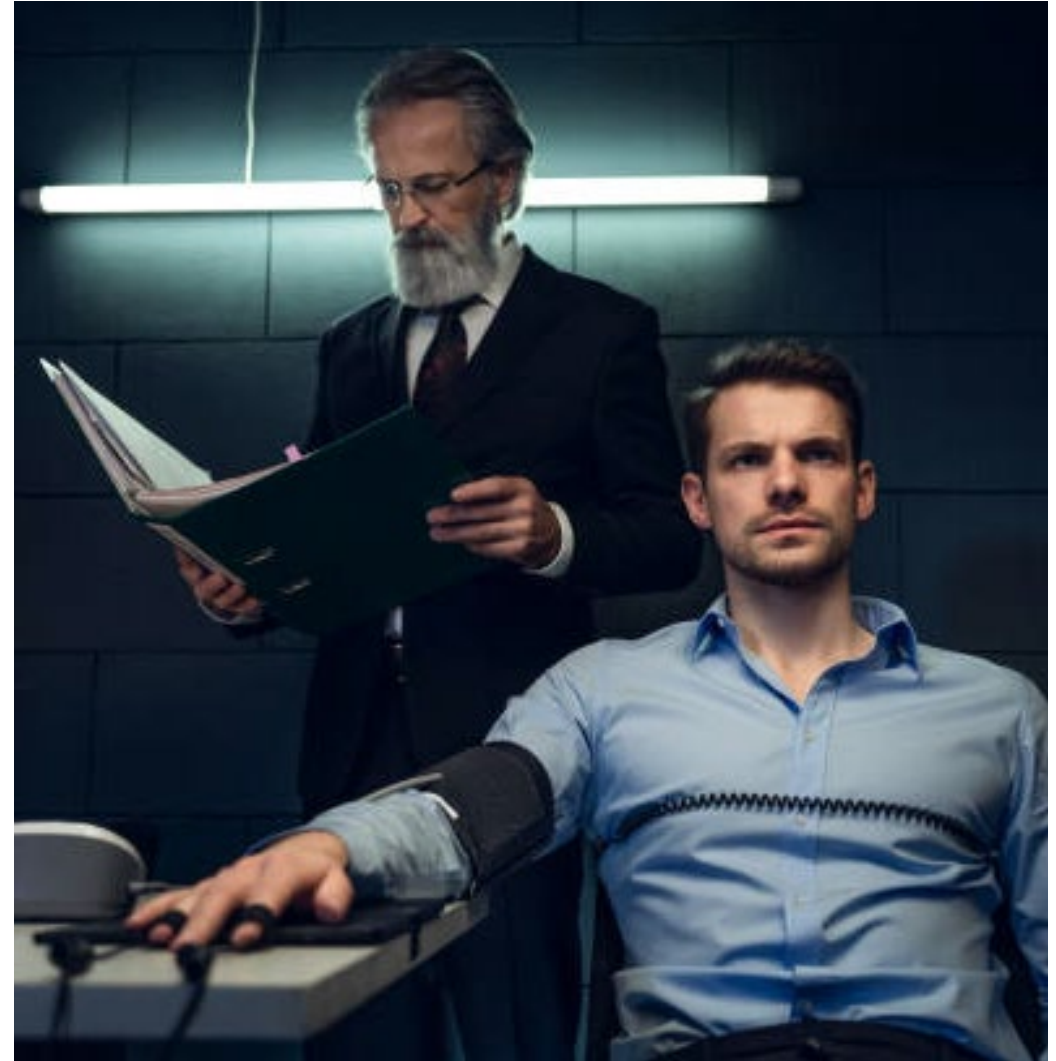
- Investigation revealed credit card payments to four businesses without supporting documentation.
- Day after request for additional documentation, management analyst took an unexpected leave.
- CFO was unable to find any supporting documentation for the expenses.
- The businesses were registered with the state using the analyst's name and home address.





# Poll #5: How was the fraud / loss detected?

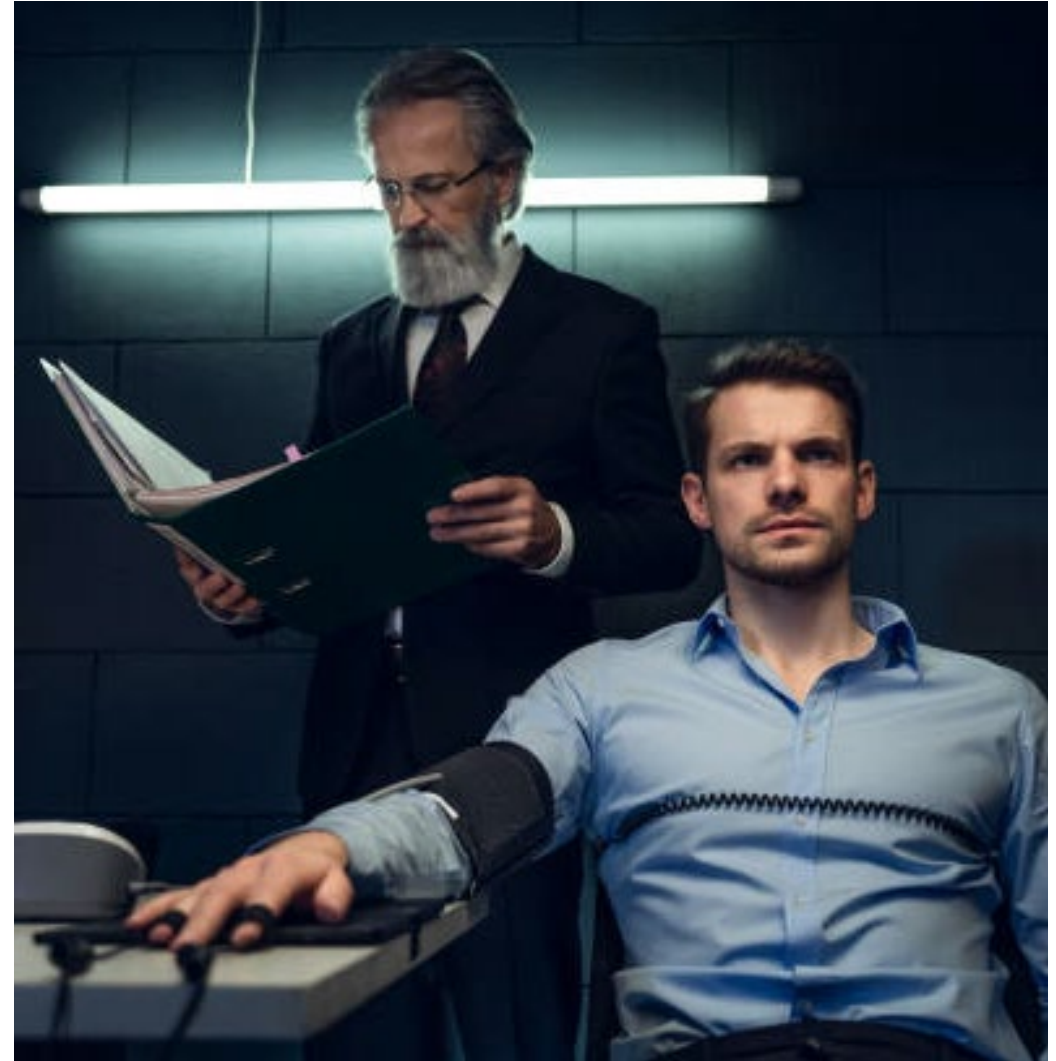
1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens



# Poll #5: How was the fraud / loss detected?

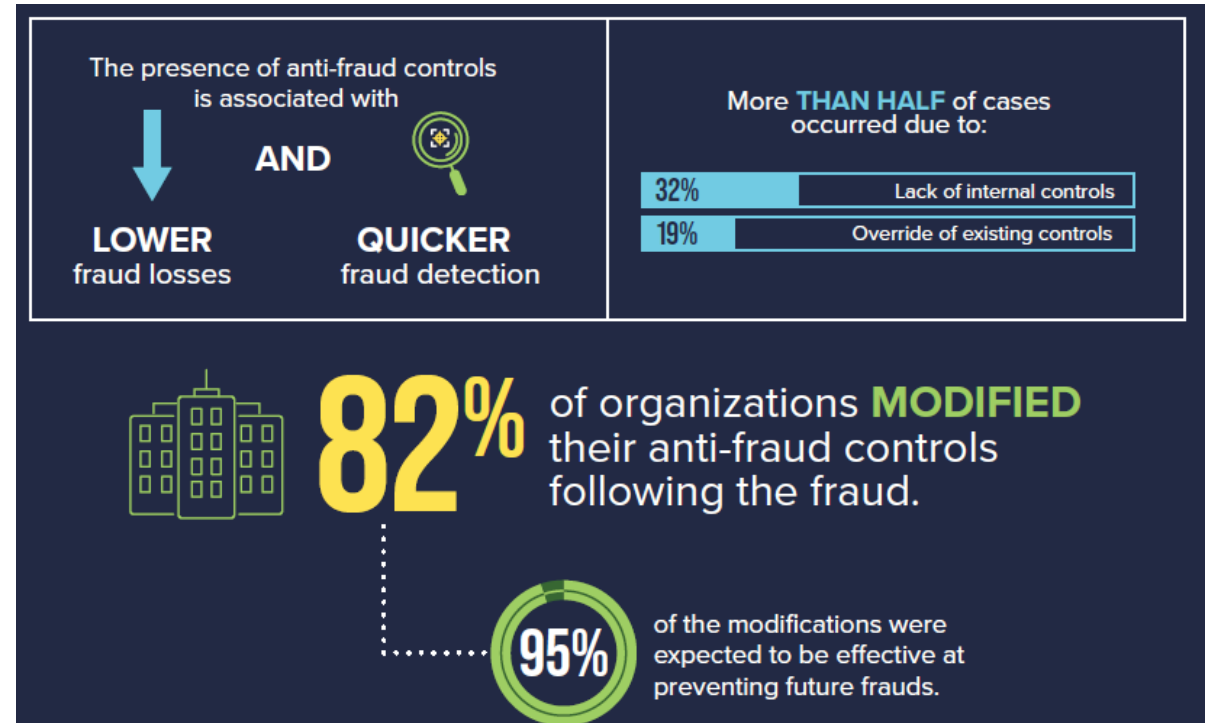
---

1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. **Third line of defense: Audit**
4. Other parties: whistleblowers, customers, concerned citizens



# Case #5: Discussion

- Incompatible duties
- circumvent multiple types of controls
- Where was the monitoring?



# Case #6: City of Zillah

---

An investigation found at least \$3,239 in public funds misappropriated from Municipal Court between September 2021 and August 2023.

Additionally, \$2,608 in questionable activities were identified between April 2021 and August 2023.



# Case #6: Background

---

Some Court payments are made via a secure drop box.

- Two staff collect and record Dropbox payments received.
- The court administrator deposits the receipted payments.
  - The municipal court administrator was responsible for sending delinquent accounts to collections monthly.
  - The administrator had system access that allowed her to post payments and to adjust customer accounts.



# Case #6: How the Fraud / Loss Occurred

---

- The investigation revealed no accounts had been sent to collections since May 2022.
  - Court had 83 accounts with outstanding balances totaling \$43,507.
- After outstanding collection letters were mailed, several people said they had previously paid their balances and would provide written declarations attesting to this.



# Case #6: How the Fraud / Loss Occurred

---

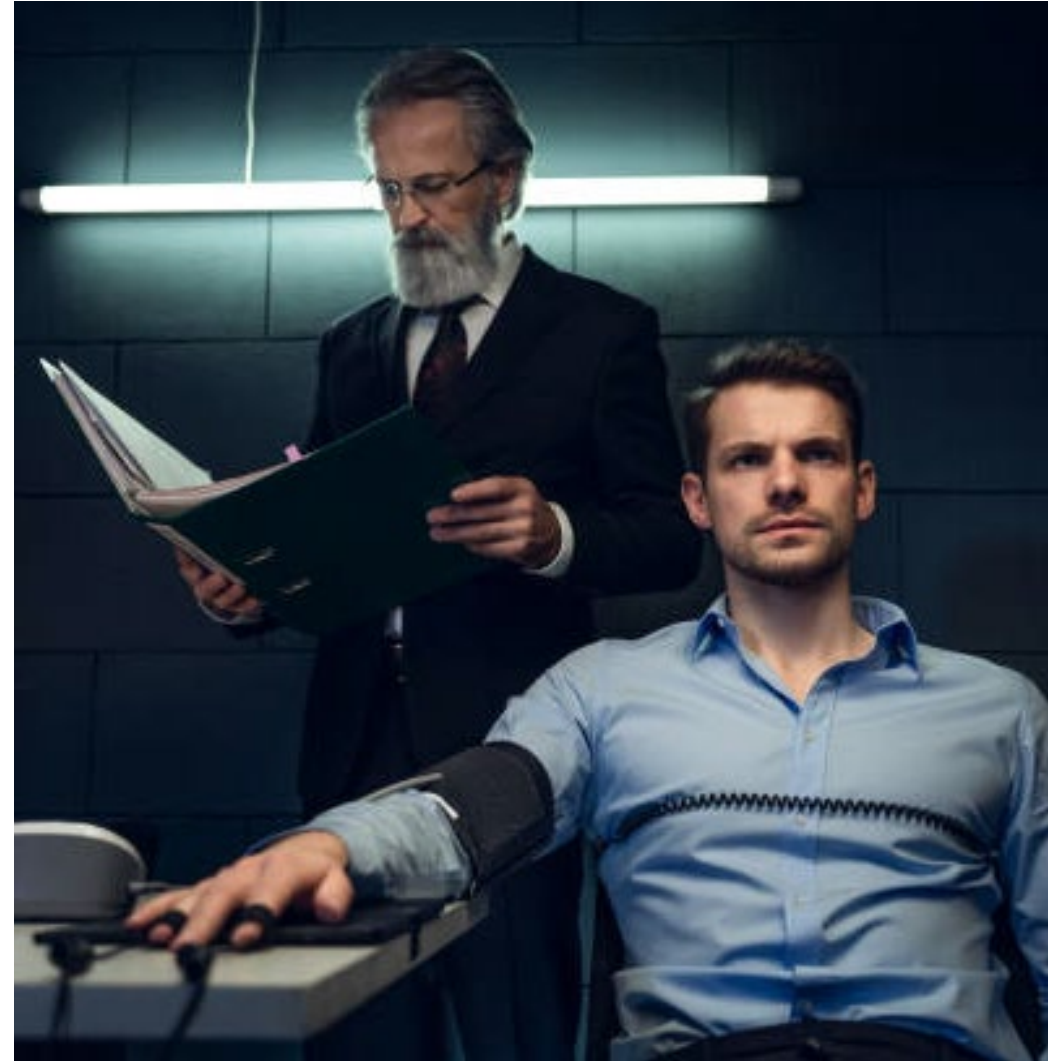
- Court Payment Tracker, a written log detailing drop box payments, was missing for all months prior to April 2023.
- Adjustments were made to court accounts that appeared unusual and were coded as “errors.”
- City established an independent review of adjustments, but it was ineffective
- August 2023: Court Admin fired for other performance reasons



# Poll #6: How was the fraud / loss detected?

---

1. First line of Defense: control activities
2. Second line: information and communication, monitoring
3. Third line of defense: Audit
4. Other parties: whistleblowers, customers, concerned citizens





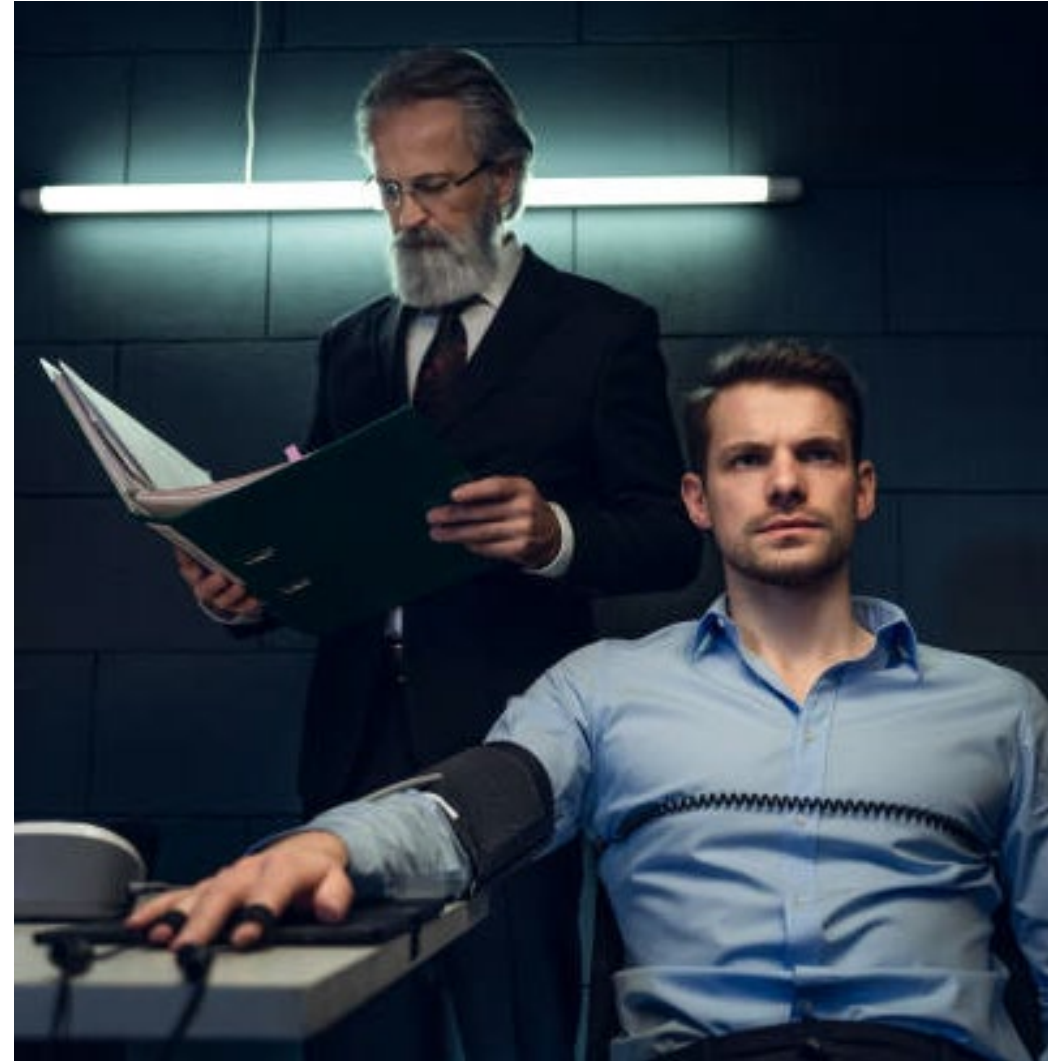
# Poll #6: How was the fraud / loss detected?

1. First line of Defense: control activities

2. Second line: information and communication, monitoring

3. Third line of defense: Audit

4. Other parties: whistleblowers, customers, concerned citizens



# Case #6: Discussion

- Existing control was ineffective
- Importance of understanding why
- Red Flag: performance issues / errors



## 3 Takeaways from Today

---

1. The first presentation focused on **RISK**. If one of your fraud risks was realized, how long would your system of controls take to detect it?  
*Would it detect it at all?*
2. Systems of internal control are more effective when we understand why
3. Professional skepticism is one of the most effective anti-fraud tools



# Thank you!

## Comments and questions

Clark County Public Service Center

1300 Franklin Street • PO Box 5000

Vancouver, WA 98666-5000



# Clark County Fraud Seminar

Internal control resources from the Office of the Washington State Auditor

Niles Kostick, Manager  
Center for Government Innovation

December 2024



Center for Government  
**Innovation**

# The Center for Government Innovation

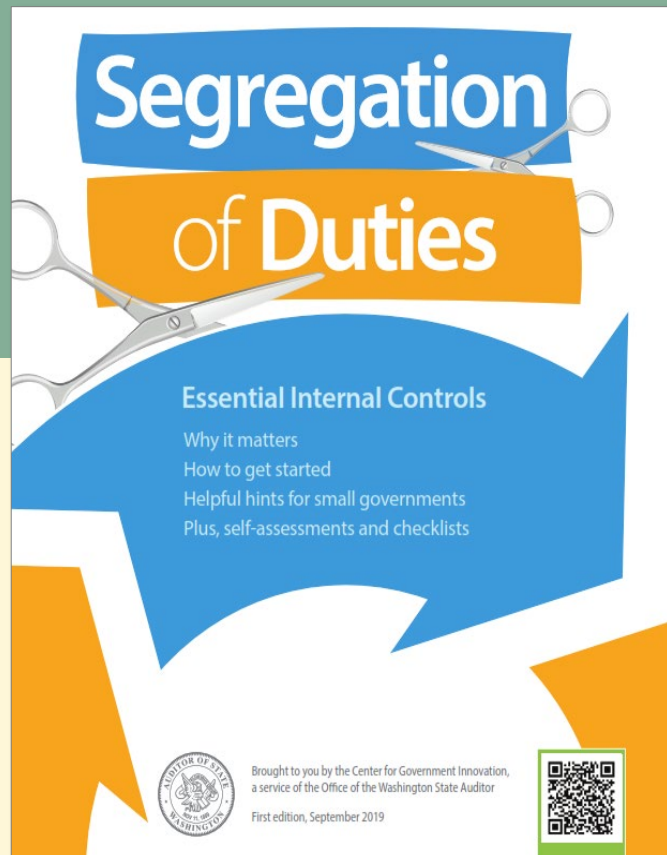
- **Resource Library** provides tools, checklists and other resources to improve internal controls, compliance and other operational areas
- **Cyber checkups** helps WA governments assess vulnerabilities to common cybersecurity threats.
- **Customized Lean facilitations & trainings** helps WA governments improve how work gets done.
- **Teambuilding workshops** helps WA governments strengthen teams, increase trust and promote workplace harmony.
- **Financial Intelligence Tool (FIT)** helps any user assess a local WA government's financial health.



# A look at fraud in Washington




# Where to get started...

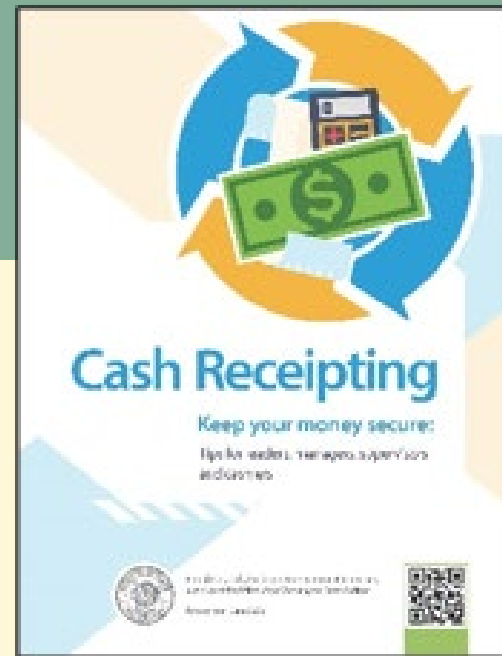



**Segregation of Duties**

**Essential Internal Controls**


- Why it matters
- How to get started
- Helpful hints for small governments
- Plus, self-assessments and checklists

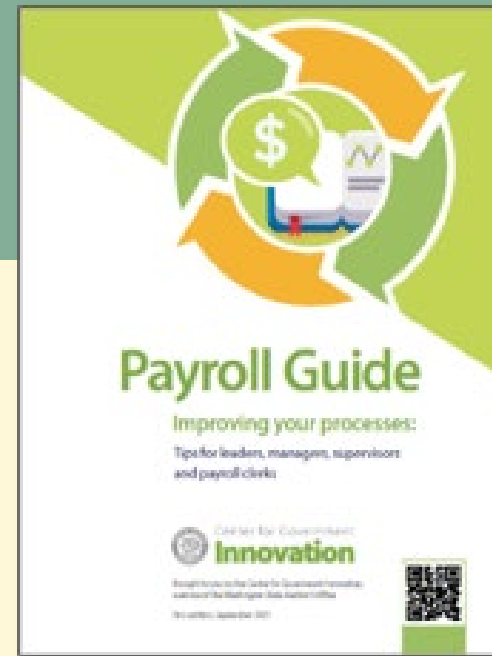

 Brought to you by the Center for Government Innovation, a service of the Office of the Washington State Auditor  
First edition, September 2019



**Cash Receipting**


Keep your money secure:  
Tips for leaders, managers, supervisors and payroll clerks

 Brought to you by the Center for Government Innovation, a service of the Office of the Washington State Auditor  
November 2018

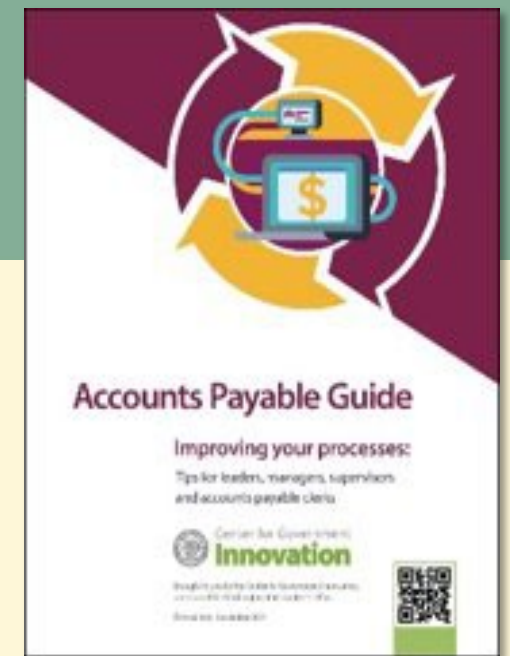



**Payroll Guide**

Improving your processes:  
Tips for leaders, managers, supervisors and payroll clerks


 Center for Government  
**Innovation**

Brought to you by the Center for Government Innovation, a service of the Office of the Washington State Auditor  
First edition, September 2019




**Accounts Payable Guide**

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

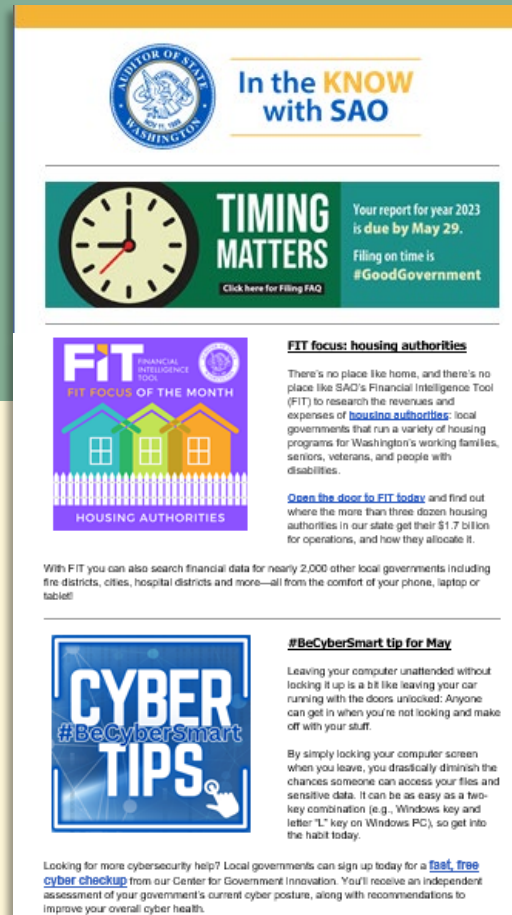
 Center for Government  
**Innovation**

Brought to you by the Center for Government Innovation, a service of the Office of the Washington State Auditor  
November 2018





# Subscribe to SAO's e-newsletter



The screenshot shows the top portion of an e-newsletter. At the top left is the Auditor of State of Washington logo. To its right is the text "In the KNOW with SAO". Below this is a "TIMING MATTERS" section featuring a clock icon and the text "Your report for year 2023 is due by May 29. Filing on time is #GoodGovernment". The next section is titled "FIT focus: housing authorities" and includes a graphic of three houses. The text discusses the SAO's Financial Intelligence Tool (FIT) and its use in researching housing authorities. Below this is a "CYBER TIPS" section with a graphic of a computer screen and the text "#BeCyberSmart". The bottom of the screenshot shows a link to a "fast, free cyber checkup" service.

Two ways to sign up:

1. Via SAO's website at [sao.wa.gov](http://sao.wa.gov)
2. Scan the QR code below:



# “They help governments get what they want.”

- Fiscal accountability & trust
- Compliance with regulations, laws, restrictions
- Preventing, deterring & detecting fraud
- Efficiency & effectiveness
- Safeguarding assets



## Importance of internal controls



# Segregation of duties

- Process or department approach, not always a government-wide approach
- Look both up- and down-stream for decentralized processes or locations
- Use a risk assessment, document controls and aim for continuous improvement



## Importance of internal controls

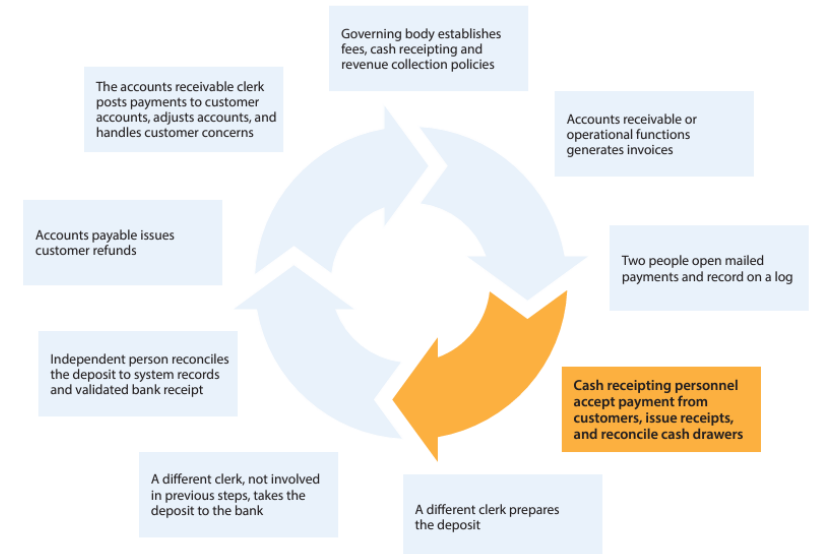


# Segregation of duties

**Table 1** – If the employee’s job is to receive payments and produce receipts for customers, or have other access to money, whether cash or checks, for deposit, then:

Other roles this employee should not have	The risk if the employee does both roles	The compensating controls you could put in place include
<p><b>Issuing receipts without supervision</b></p>	<p><b>Skimming schemes.</b> One version involves taking cash before it has been recorded or before issuing a receipt for the payment.</p> <p>Another trick involves using a manual or unauthorized receipt book, to hide the funds that are pocketed.</p> <p><b>Note:</b> Risk for such schemes is lower when all cash intake is expected. However, even in these settings, unexpected or miscellaneous revenues can be at risk.</p>	<ul style="list-style-type: none"> <li>• Place surveillance cameras on receiving operations</li> <li>• Place signs telling customers to expect a receipt, and urging them to contact a manager if they have concerns</li> <li>• Use cash drawers that capture zero receipts (drawer was opened but no receipt was given)</li> <li>• Monitor the daily deposit for reasonableness, in total and amount of cash</li> <li>• Conduct surprise cash counts, and look for unauthorized receipt books during the count</li> <li>• Put in place additional controls to monitor unexpected revenue streams</li> <li>• Conduct an internal audit test: Have an auditor pose as a customer, pay in cash, and not ask for a receipt. Assess whether the funds are properly recorded and the cashier insisted on providing a receipt.</li> <li>• Monitor inventory for unexplained shortages</li> </ul>

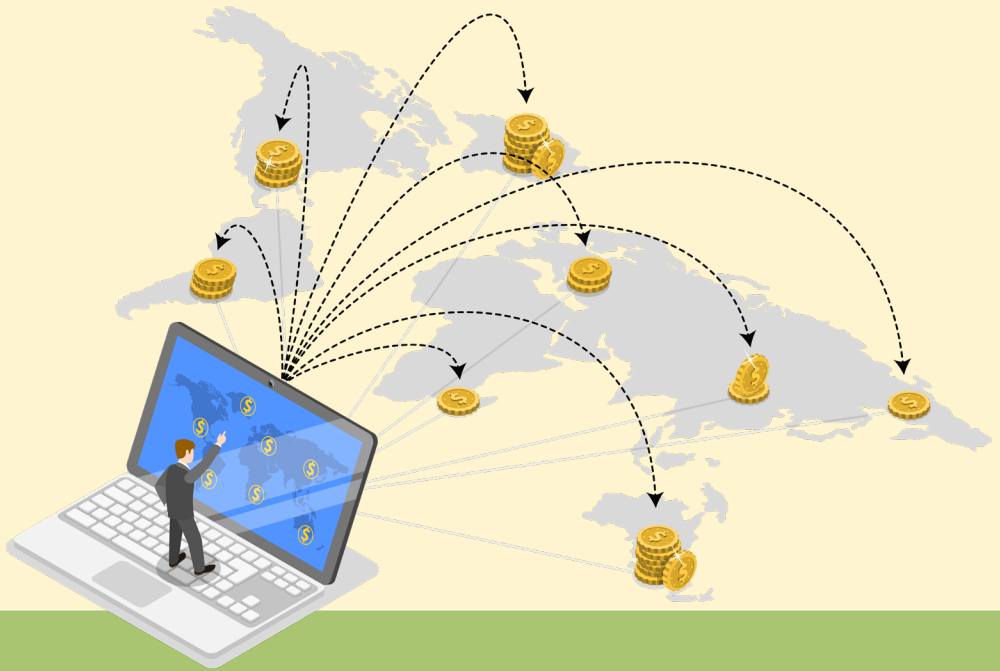
**Diagram 1** – Cash receiving roles



# Segregation of duties

	Question	Are duties segregated? Yes or No	Risk tolerance (see cell comment)	Describe compensating controls (CC) in place that address the risks	Are your controls adequate?	Describe whether you will add any controls OR segregate this duty
<b>Examples</b>						
	<i>Do cashiers have complete control over issuing receipts? For example, could they issue an unauthorized receipt or not give a customer a receipt and pocket the money undetected?</i>	No	Very low	<i>We have a sign telling customers to expect a receipt at the park entrance</i>	No	<i>We will add a requirement that the customer place the receipt on their vehicle dash and will tow vehicles without it</i>
	<i>Can cashiers also void receipts or process refunds to customers?</i>	Yes				
<b>Section 1. Cash Receipting</b>						
1a	Do cashiers have complete control over issuing receipts? For example, could they issue an unauthorized receipt or not give a customer a receipt and pocket the money undetected?					
1b	Can cashiers also void receipts or process refunds to customers?					
1c	Do cashiers who receipt in-person cash or check payments also open payments that come through the mail?					
1d	Can cashiers generate or modify the billings for goods or services?					





# Prevention and detection reviews

**Attorney General suing city official after auditor's report finds ethics violation**

**Former clerk-treasurer charged with theft**

**Former mayor sentenced to 90 days in jail**



## Avoid the trusted employee trap:

- No segregation of duties
- Inadequate monitoring & review

**Trust is not an  
internal control**





Trust is not an  
internal control

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





# Survey says...

What percentage of fraudsters are first-time offenders?





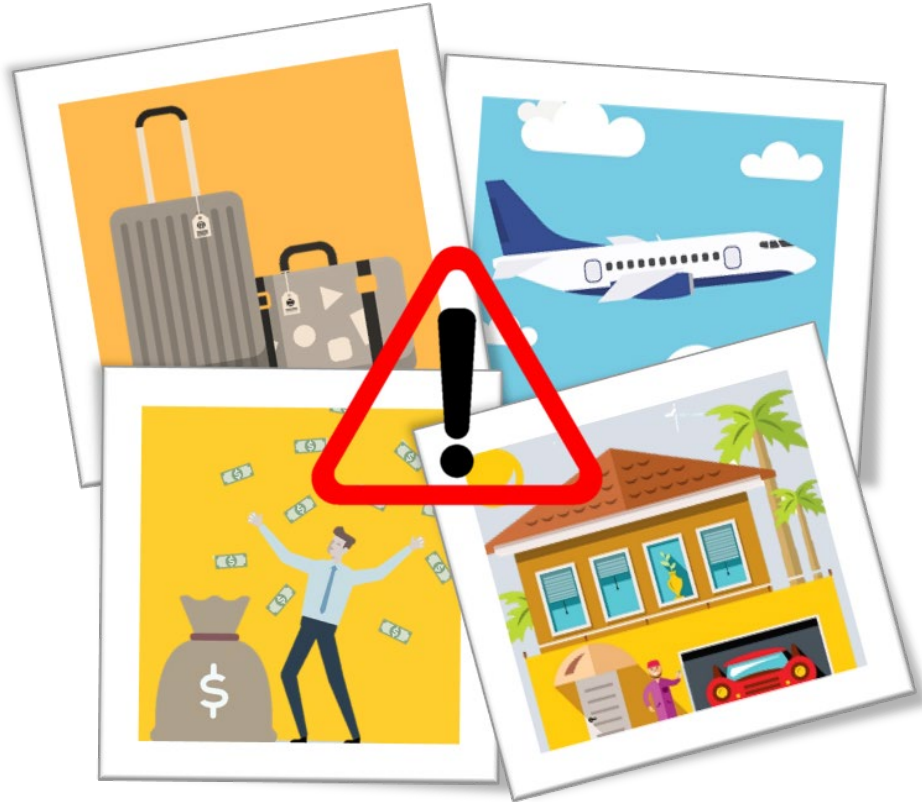
**Trust is not an  
internal control**

## Abuse of positions

Fraudster intentionally abuses the responsibilities of their position to manipulate financial transactions to attain personal or financial gain.



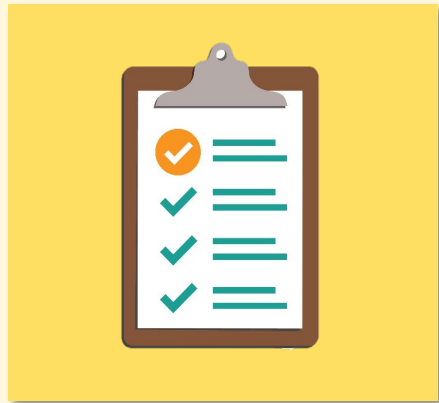
# Know the warning signs



- Refusing to take vacation
- Unwillingness to share duties
- Working long or odd hours
- Changing work patterns
- Living beyond their means
- Experiencing financial difficulties

# Types of internal controls

## Preventative



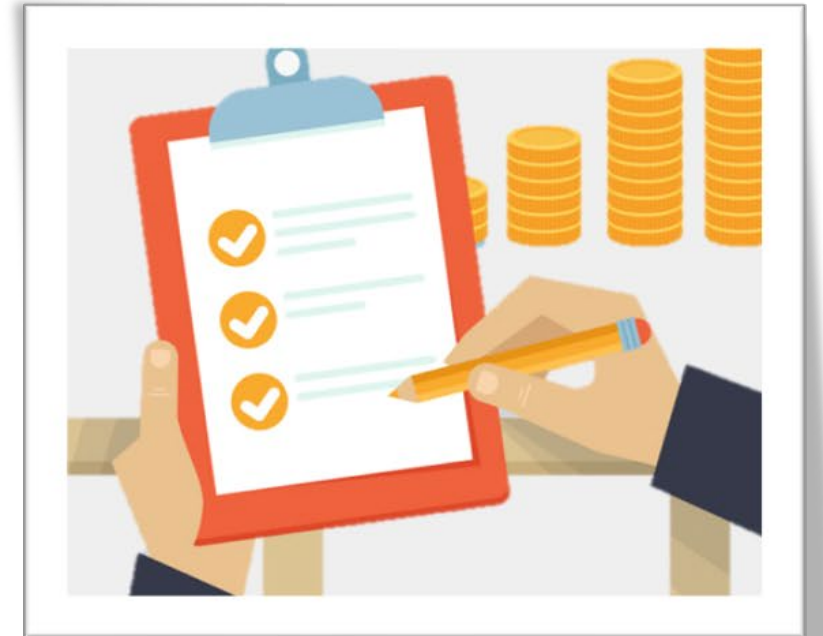
- ✓ Define process
- ✓ Develop expectations
- ✓ Develop forms & reports

## Detective



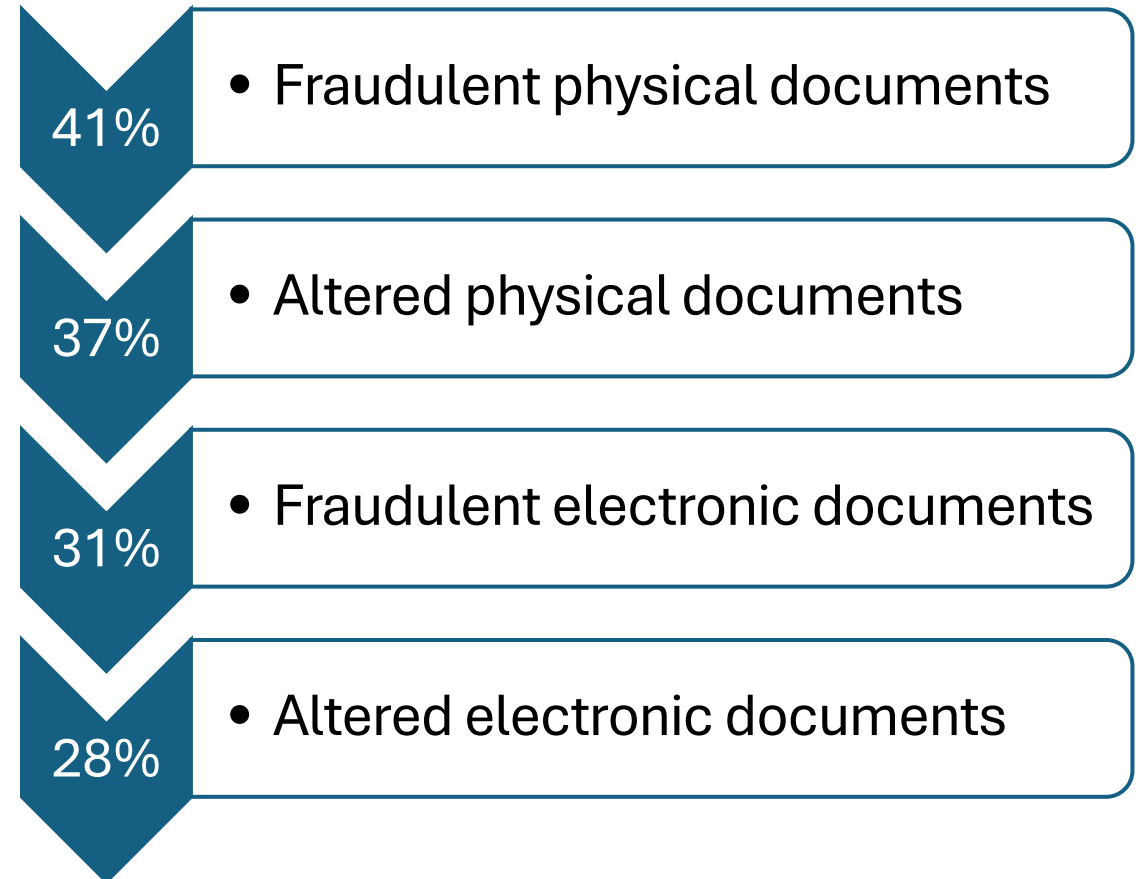
- ✓ Review documents
- ✓ Observe & monitor activities

# Standardize forms and reports

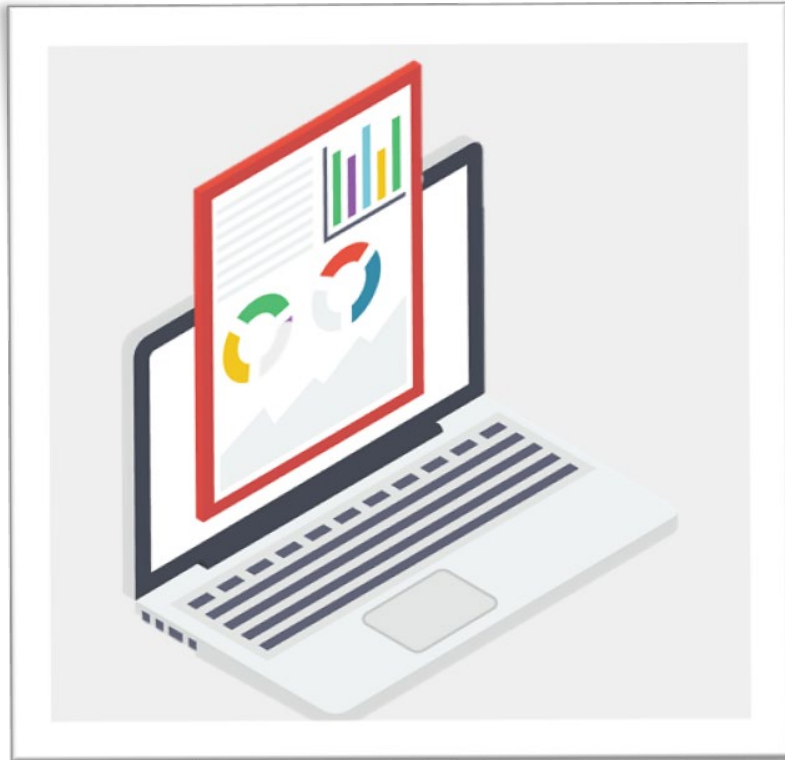


# Forms and fraud

In **89%** of reported cases, fraudsters manipulated records or forms to conceal fraud



# Minimize the risk of error or manipulation



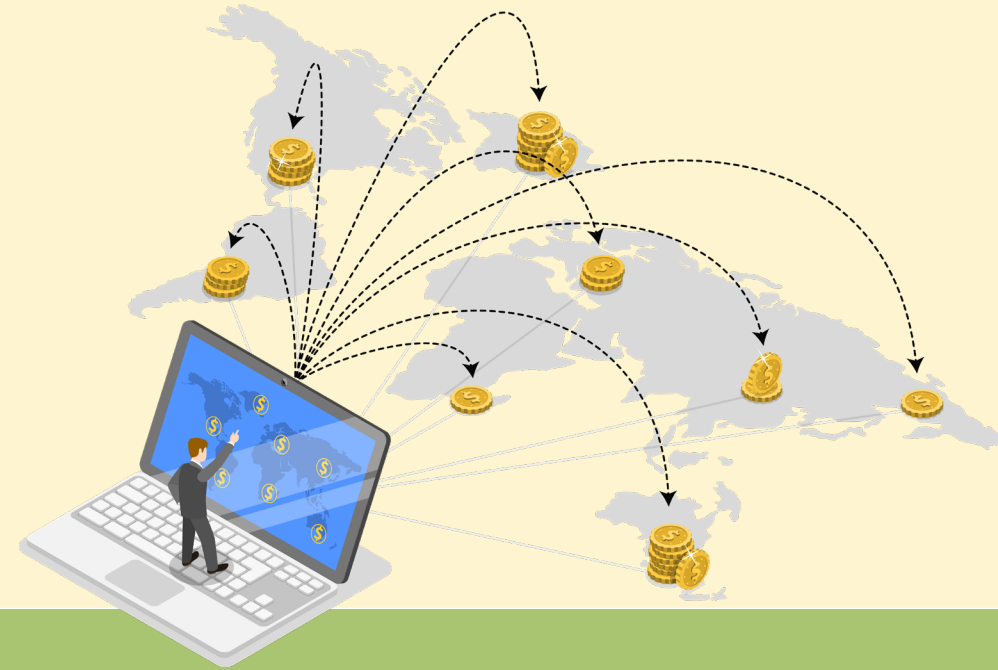
Require system generated reports for review. Pull source documents and statements instead of those used by the preparer. Restrict editing to spreadsheets if they are necessary.



**Hundreds of county residents linked to recent data breach**

**Port loses \$500,000 in public funds to cyberfraud**

**City paid \$185,897 to fraudulent vendor**



**Electronic payments and cyber loss**





**Bad actors manipulate  
our trusting human  
nature to perpetrate  
their attacks**



**How do cyber  
threats happen**




## How bad is it?

**\$2.9 billion** in losses

**\$3.4 billion** emails sent every day

**91% of breaches** begin with phishing emails to an employee



# How do cyber threats happen



# Threat trend – account takeover

**Improper use of valid logins/accounts via compromised credentials**

It's easier to login than hack.




## How do cyber threats happen



# Threat trend – targeting backups

**Removing the primary response to an attack.**

Leads to higher and more successful ransom payments




## How do cyber threats happen



# Threat trend – targeting infrastructure

## Maximizing disruption

Physical infrastructure + technology.  
Think of your utilities, physical payment systems, etc.




**How do cyber threats happen**



# Threat trend – generative AI

## Creating a more convincing fakes

Phishing attempts look & sound just like colleagues.



How do cyber  
threats happen



# Cyber incident reports to SAO

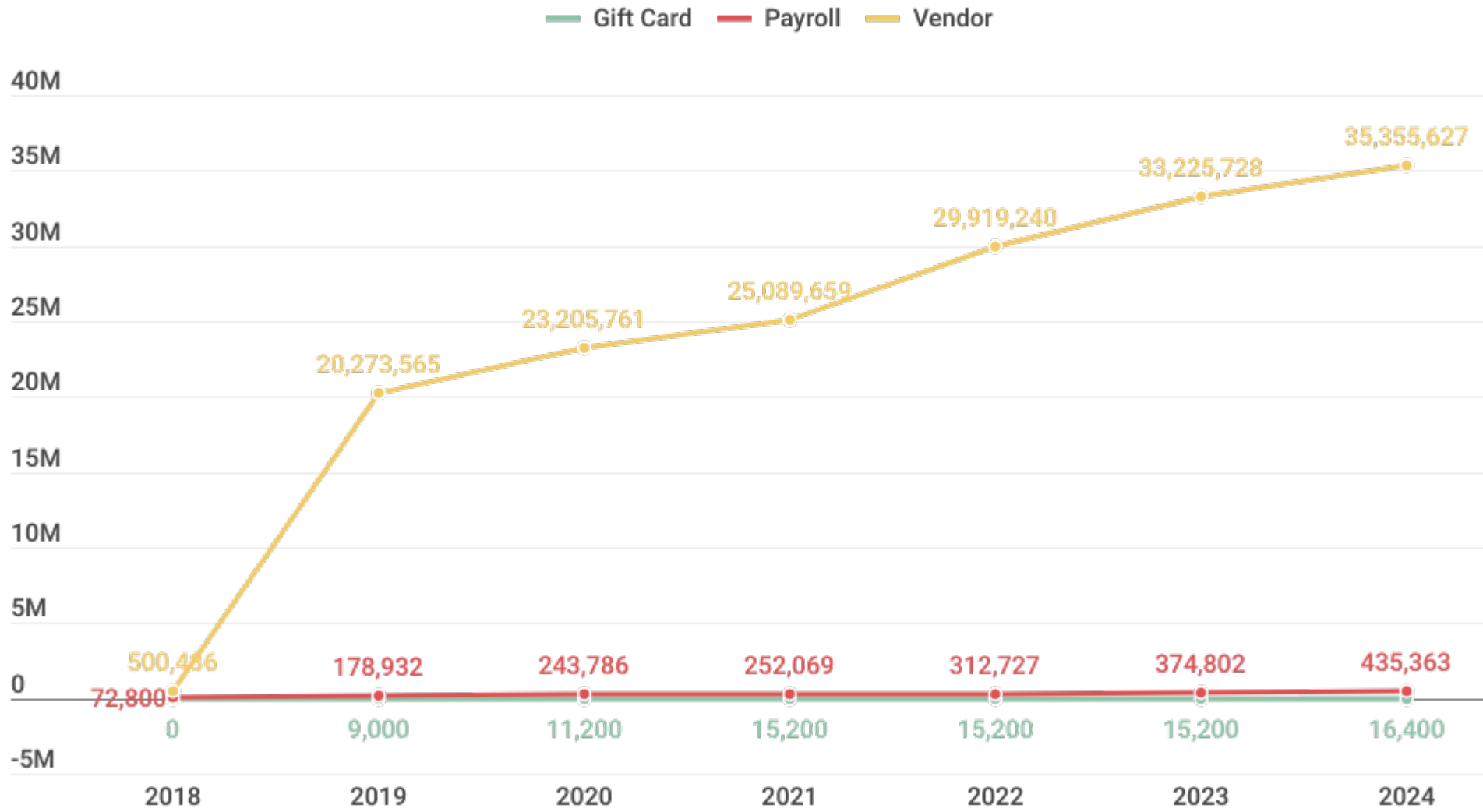


**182** cases submitted since 2018

**\$36 million** in total losses

**50+ governments** reported being successful targets in the last two years





Cyber loss - losses





# Financial controls help ward off cyber criminals

## Strong written policies

- Standardized process to initiate, approve and execute transactions
- Additional segregation of duties for changes to vendor or payee information
- Require reporting of suspicious activity immediately
- Go to the source – your vendor's official email/phone numbers



# How to prevent it



# Financial controls help ward off cyber criminals

## Best practices

- Require two to execute ACH
- Segregate duties:

Process A/P

Process A/P

ACH processing

Should not edit vendor files

Should not create / handle / approve ACH

Should not prepare bank reconciliations



# How to prevent it



# Educate employees to be responsibly suspicious

## Slow down

- Consider the source
- Question the unusual
- Know the red flags



# How to prevent it



# Educate employees to be responsibly suspicious

- Start a new email chain
- Use reliable contact information
- Scrutinize emails requesting payment or changes to accounts
- Require notifications of account changes before they happen using multiple channels



## How to prevent it



# Build a skeptical cyber culture

CYBERSECURITY  
is everyone's job.

**Leadership and Planning**


## It starts with policy

A guide to jump-starting your cybersecurity program

The State Auditor's Office launched the Cyber Checkup program in 2023, and one of the common results we found from this program 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.



  Office of the Washington State Auditor  
Pat McCarthy  
August 2024

CYBERSECURITY  
is everyone's job.

**Finance and Administration**

## 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  
Updated July 2023

## By role:

- Leadership
- Finance
- Facilities & Ops
- HR
- Information Technology
- Legal

# Information

**Niles Kostick, Manager**

SAO's Center for Government Innovation

[Center@sao.wa.gov](mailto:Center@sao.wa.gov)

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

Twitter: [www.twitter.com/WaStateAuditor](http://www.twitter.com/WaStateAuditor)

Facebook: [www.facebook.com/WaStateAuditorsOffice](http://www.facebook.com/WaStateAuditorsOffice)

