

# THE BONADIO GROUP

CPAs, Consultants & More

## Understanding Fraud Risks and Fraud Prevention Strategies

**Presented by:**  
**Timothy Ball, CFE**  
**Brian Lafountain, CPA, CFE**

# Overview

I. Types of Fraud

II. The Fraud Triangle

III. Which Employees Steal

IV. Fraud Detection & Victim Organizations

V. Most Common Types of Fraud

VI. Red Flags of Fraud

VII. COSO Fraud Risk Mgmt Guidelines

VIII. Fraud Prevention Strategies

XIV. Case Studies





## Definition

COSA defines fraud as any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

# ACFE's 2018 Global Study on Occupational Fraud and Abuse



- The typical organization loses an estimated 5% of its annual revenues to fraud
- Median loss of each individual fraud is approximately \$108,000
- About 22% of the cases involved losses of at least \$1 million

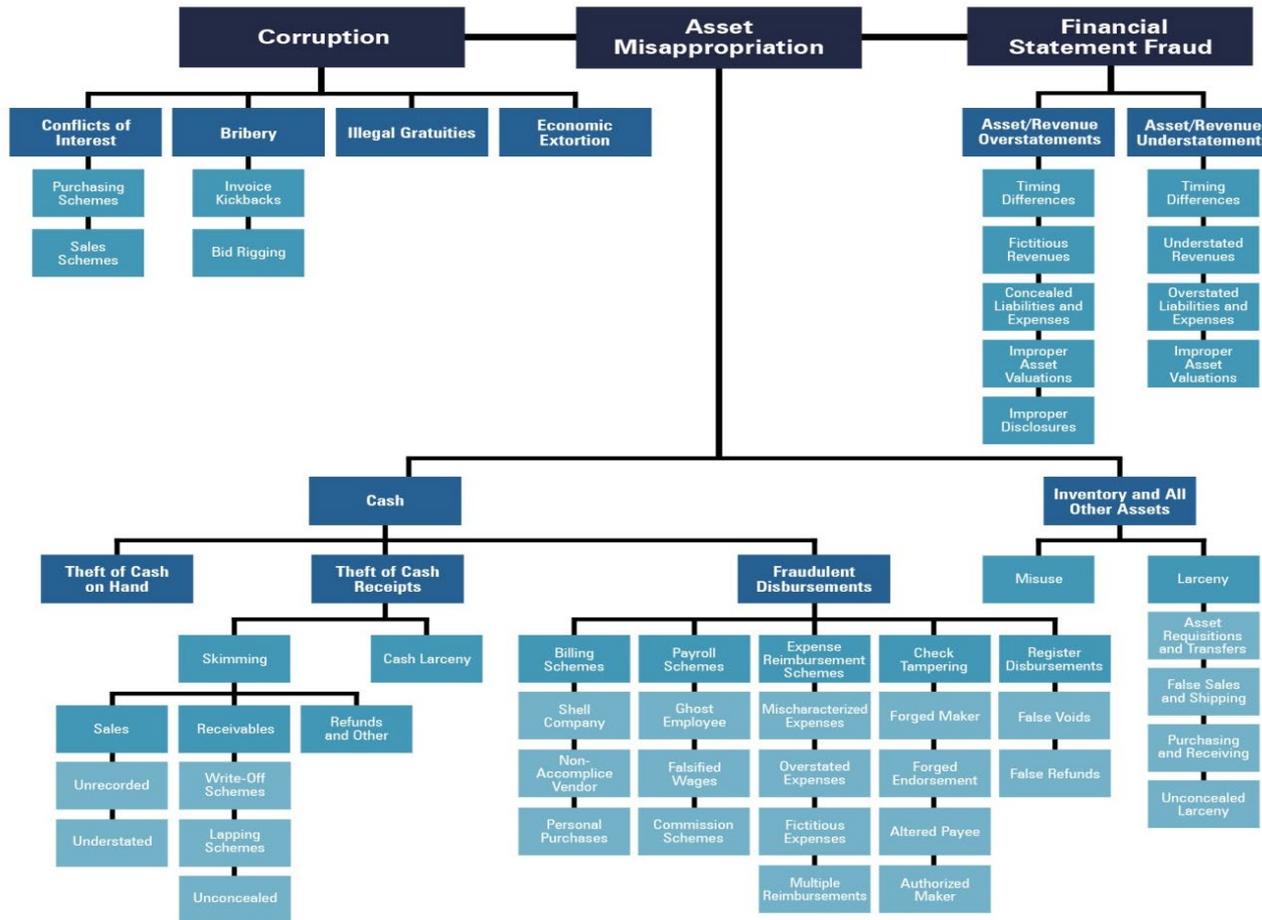
# Types of Occupational Fraud

- Financial statement fraud – 10% of frauds  
(*Wall Street Journal* cases)
- Asset Misappropriation – 89% of frauds  
(Our Main Focus for today)
- Corruption Schemes – 38% of frauds  
(Conflicts of Interest, bribery, etc. )



# Occupational Fraud Tree

Figure 3: Occupational Fraud and Abuse Classification System (Fraud Tree)



# Fraud by Region

FIG. 1 Countries with reported cases and median loss for each region



United States CASES: 1,000 (48%)  
MEDIAN LOSS: **\$108,000**



Sub-Saharan Africa CASES: 267 (13%)  
MEDIAN LOSS: **\$90,000**



Asia-Pacific CASES: 220 (11%)  
MEDIAN LOSS: **\$236,000**



Western Europe CASES: 130 (6%)  
MEDIAN LOSS: **\$200,000**



Latin America and the Caribbean CASES: 110 (5%)  
MEDIAN LOSS: **\$193,000**



Middle East and North Africa CASES: 101 (5%)  
MEDIAN LOSS: **\$200,000**



Southern Asia CASES: 96 (5%)  
MEDIAN LOSS: **\$100,000**



Eastern Europe and Western/Central Asia CASES: 86 (4%)  
MEDIAN LOSS: **\$150,000**



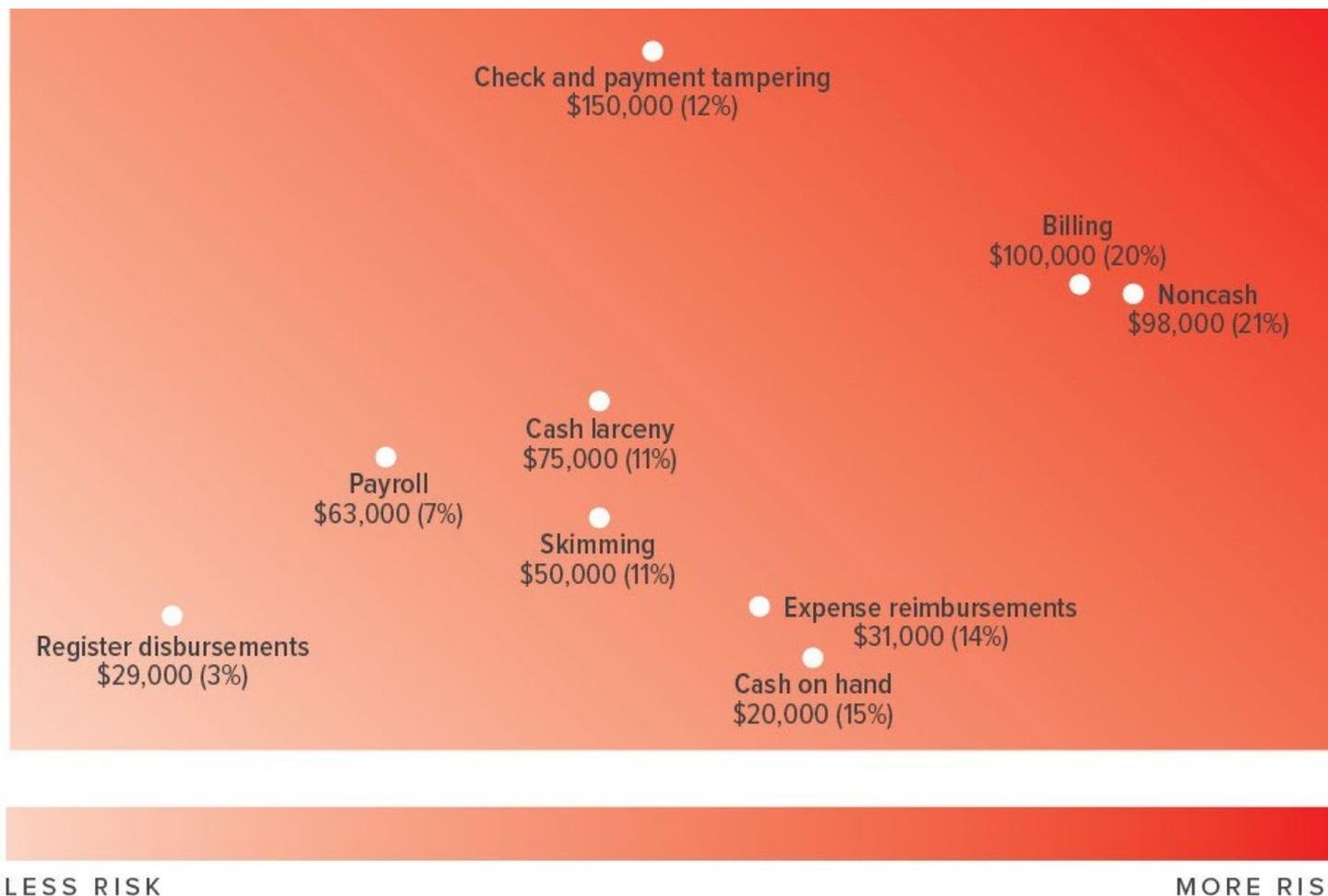
Canada CASES: 82 (4%)  
MEDIAN LOSS: **\$200,000**

# Cost of Fraud

FIG. 2 How much does an occupational fraud cost the victim organization?



# Asset Misappropriation Schemes



# Cost of Fraud

Average Armed  
Robbery  
Yields **\$250**



Average White  
Collar Crime  
Yields **\$108,000**



# Cressey Fraud Triangle

*Pressure/Motive*



*Opportunity*

*Rationalization*

# Which Employees Steal?



- Vast majority of frauds were committed by individuals in one of the following departments: accounting, operations, sales, executive/upper management, customer service, administrative support, finance or purchasing.

# Which Employees Steal?

Department*	Percent of cases	Median loss
Accounting	14%	\$ 212,000
Operations	14%	\$ 88,000
Sales	12%	\$ 90,000
Executive/upper management	11%	\$ 729,000
Customer service	8%	\$ 26,000
Administrative support	8%	\$ 91,000
Other	6%	\$ 77,000
Finance	6%	\$ 156,000
Purchasing	5%	\$ 163,000
Facilities and maintenance	3%	\$ 175,000
Warehousing/inventory	3%	\$ 200,000
Information technology	3%	\$ 225,000
Marketing/public relations	2%	\$ 80,000
Manufacturing and production	2%	\$ 200,000
Human resources	1%	\$ 76,000

# Perpetrators Position

FIG. 24 How does the perpetrator's level of authority relate to occupational fraud?



# Perpetrators Position

FIG. 25 How does the perpetrator's level of authority relate to scheme duration?

Position	Median months to detection
Employee	12 months
Manager	18 months
Owner/executive	24 months

# Perpetrator's Criminal Background

FIG. 36 Do perpetrators tend to have prior fraud convictions?



- Never charged or convicted (89%)
- Charged but not convicted (6%)
- Had prior convictions (4%)
- Other (1%)

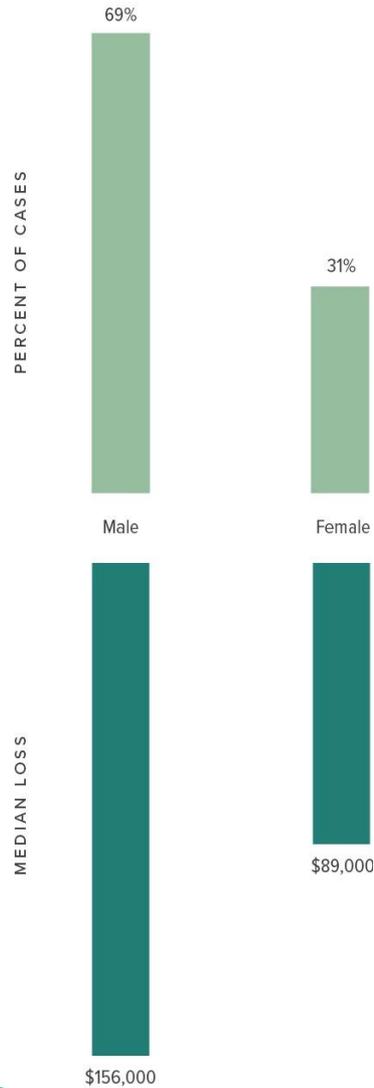
# Perpetrator's Employment History

FIG. 37 Do perpetrators tend to have prior employment-related disciplinary actions for fraud?

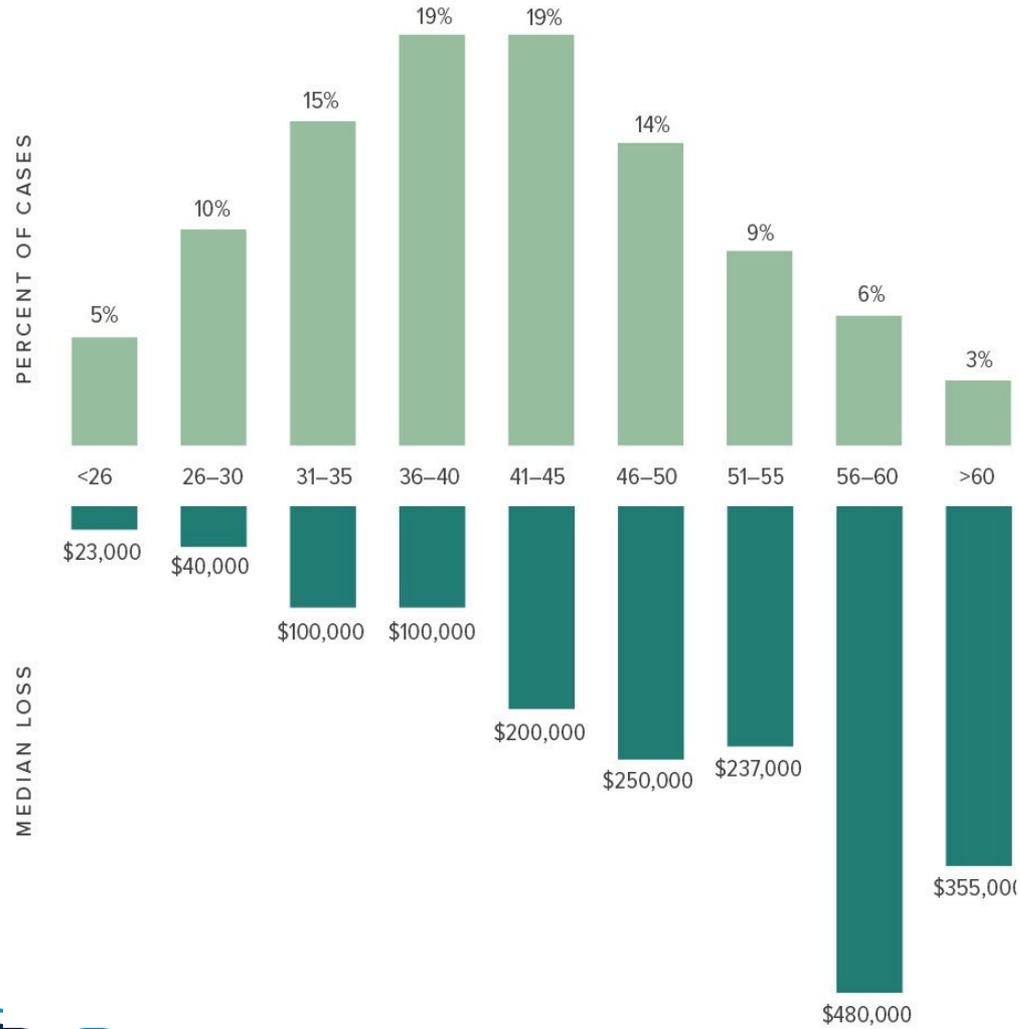


- Never punished or terminated (85%)
- Previously terminated (9%)
- Previously punished (6%)
- Other (1%)

# Perpetrator's Gender

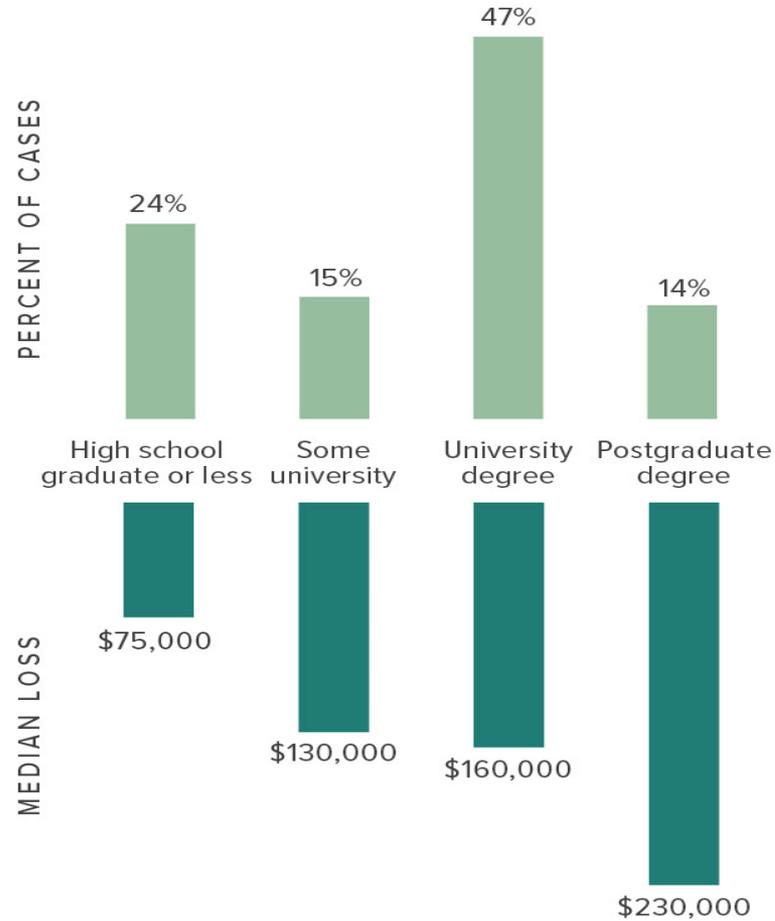


# Perpetrator's Age



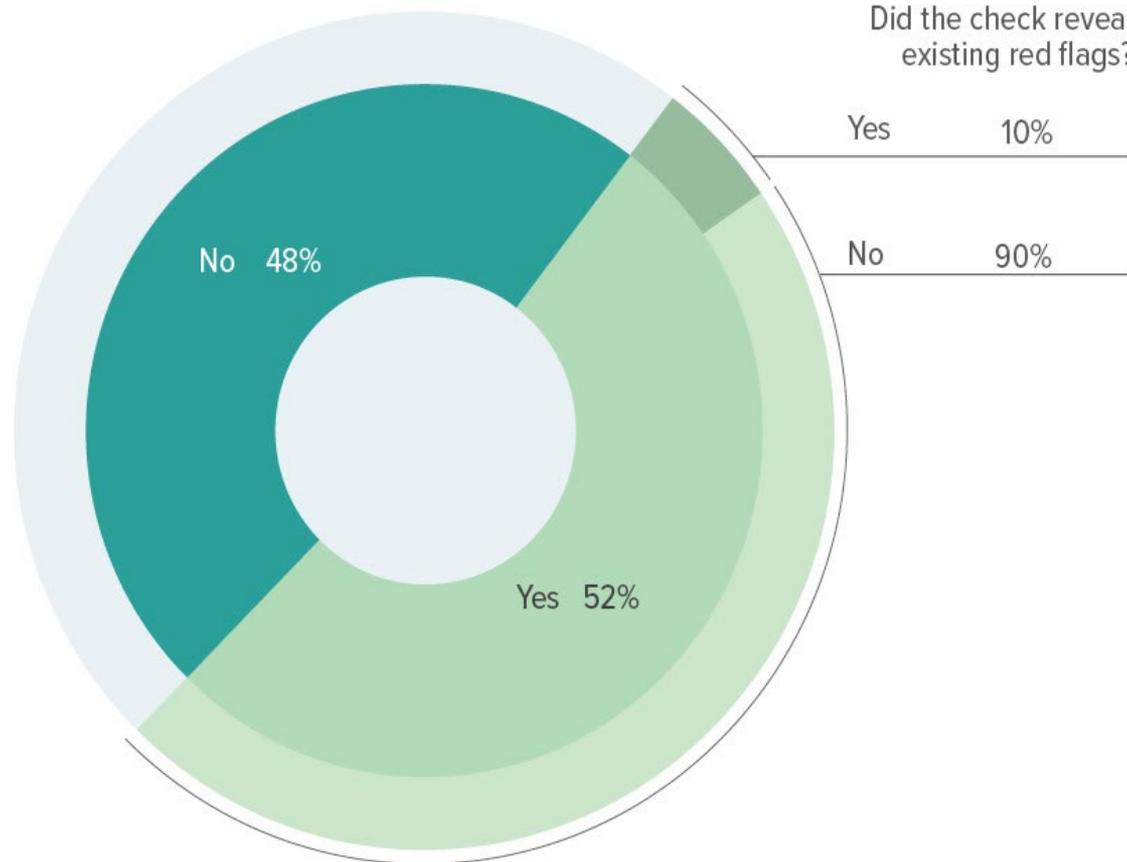
# Perpetrator's Age

FIG. 34 How does the perpetrator's education level relate to occupational fraud?



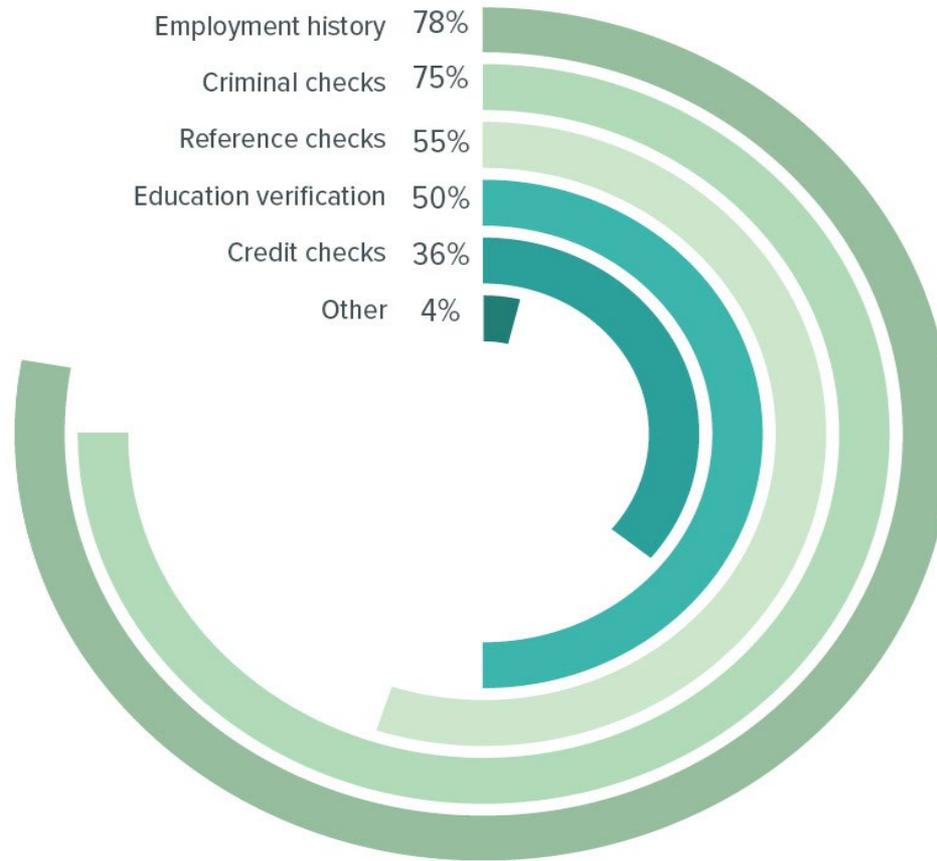
# Background Checks

FIG. 20 Was a background check run on the perpetrator prior to hiring?



# Background Checks

FIG. 21 What types of background checks were run on the perpetrator prior to hiring?



# Victim Organizations

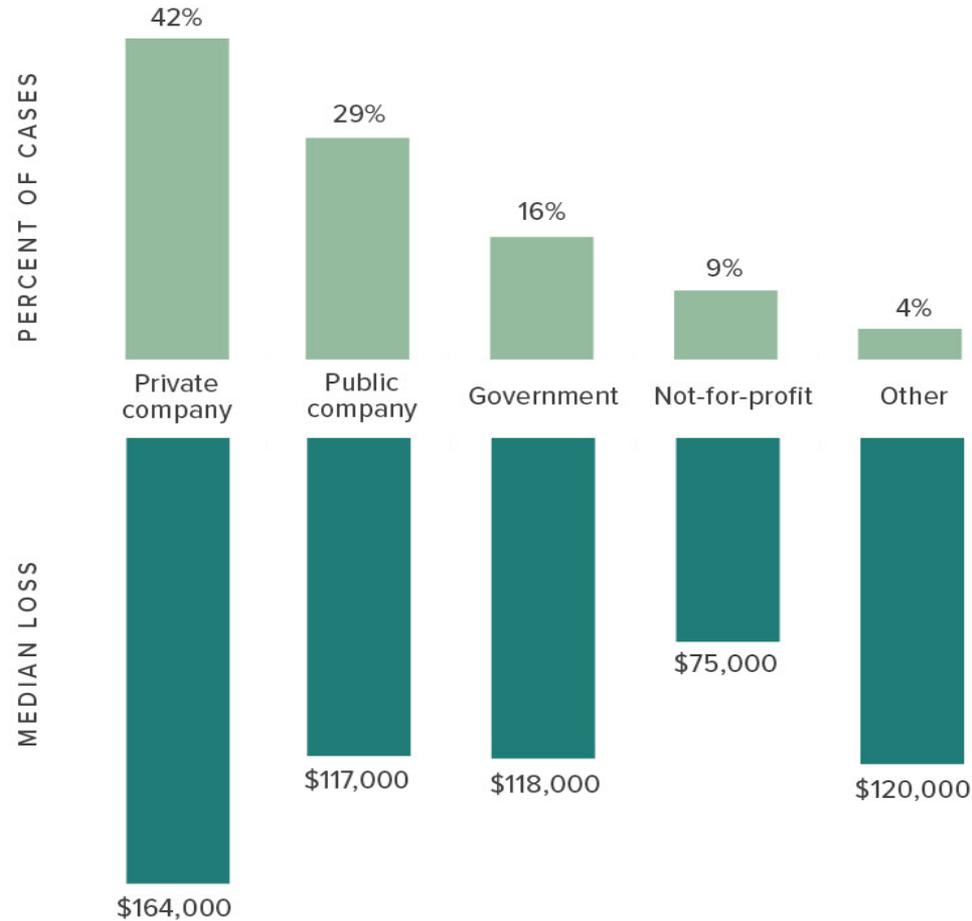


## Watch Out!

How are different kinds of organizations affected by occupational fraud?

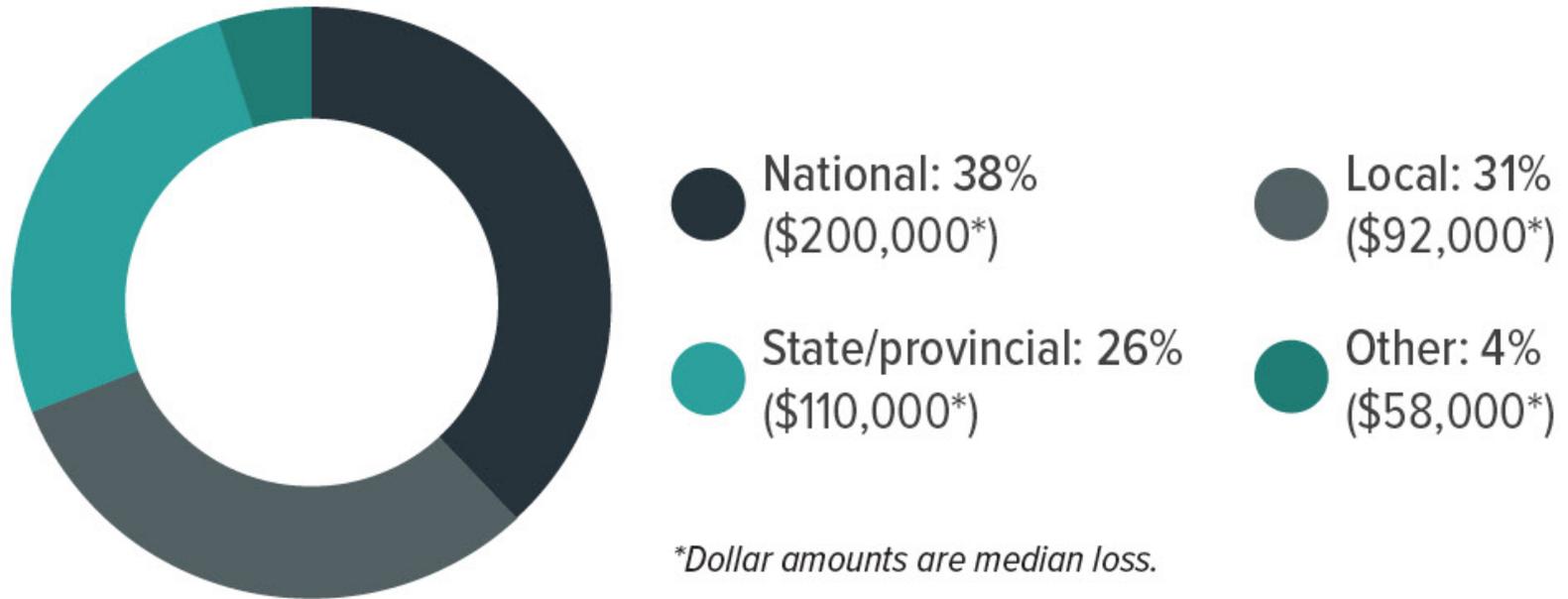
# Types of Organizations

FIG. 12 What types of organizations are victimized by occupational fraud?

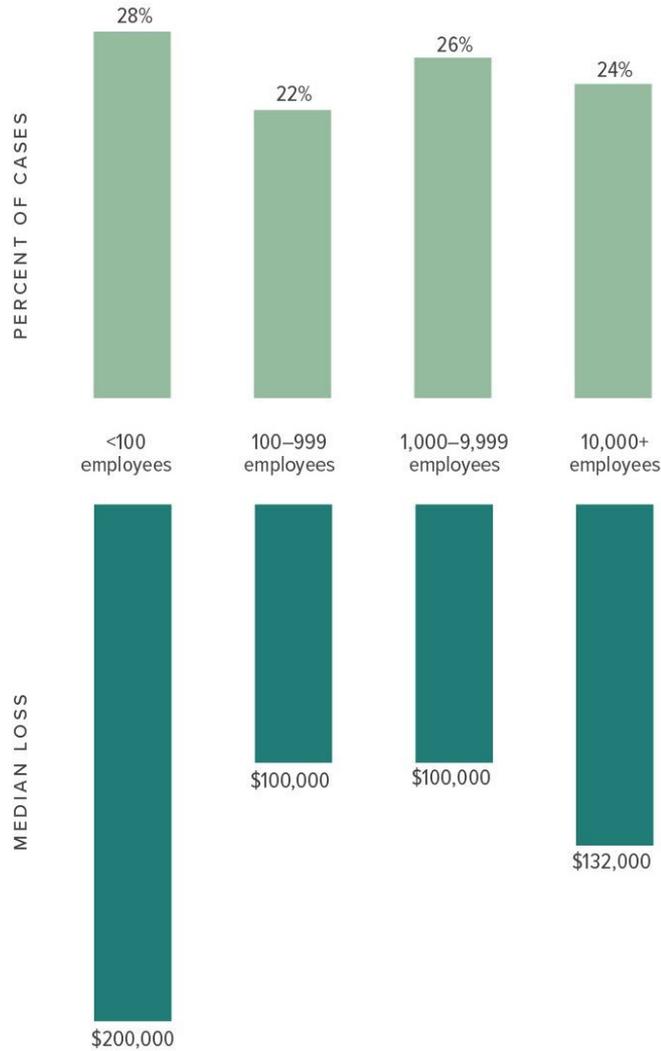


# Level of Government Organization

FIG. 13 What levels of government are victimized by occupational fraud?



# Size of Victim Organization



# Industry of Organization

FIG. 15 How does occupational fraud affect organizations in different industries?



# Most Common Schemes by Industry

INDUSTRY	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Banking and financial services	338	11%	14%	23%	12%	36%	7%	8%	11%	2%	3%	9%
Manufacturing	201	27%	8%	15%	12%	51%	18%	10%	28%	5%	3%	7%
Government and public administration	184	15%	11%	11%	9%	50%	11%	5%	22%	7%	2%	11%
Health care	149	26%	7%	13%	13%	36%	16%	11%	19%	17%	1%	12%
Retail	104	20%	10%	19%	9%	28%	8%	12%	34%	5%	13%	13%
Education	96	23%	19%	19%	6%	38%	18%	6%	19%	6%	0%	14%
Insurance	87	20%	9%	3%	18%	45%	8%	7%	11%	3%	1%	11%
Energy	86	20%	2%	10%	12%	53%	10%	3%	27%	7%	2%	10%
Construction	83	37%	12%	8%	19%	42%	23%	16%	23%	14%	1%	13%

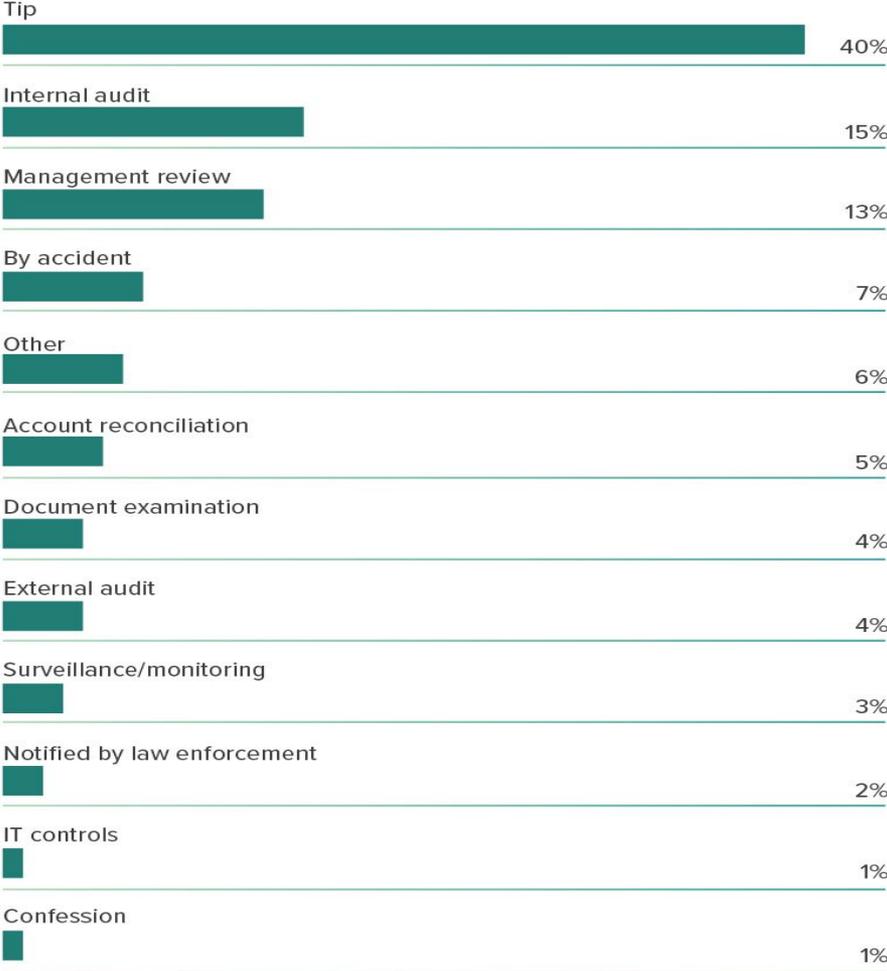
# Detection of Fraud Schemes

- External audits should not be relied upon as an organization's primary fraud detection method. Only 4% of frauds are detected through the external audit.
- While external audits serve an important purpose and can have strong preventative effect on potential fraud, their usefulness as a means of uncovering fraud is limited.



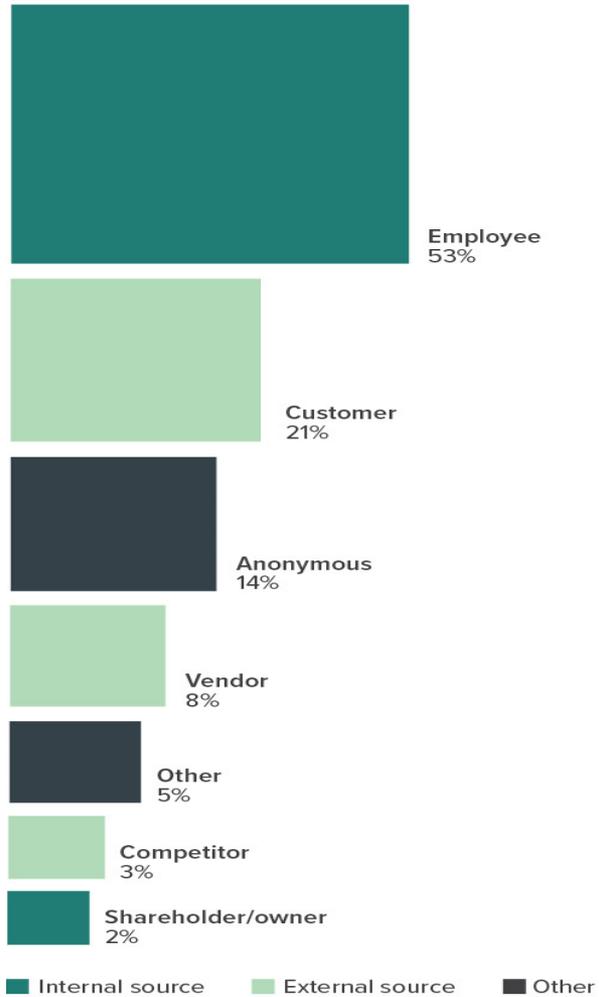
# Initial Detection of Frauds

FIG. 9 How is occupational fraud initially detected?



# Tip Sources

FIG. 10 Who reports occupational fraud?



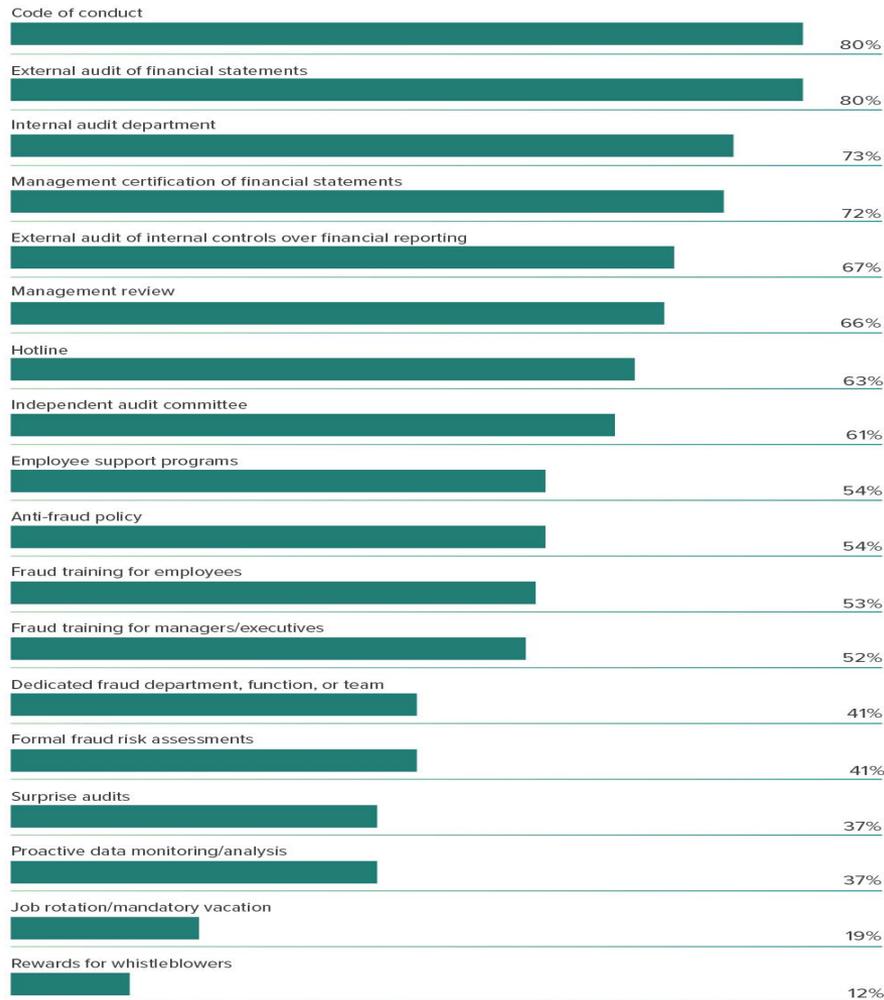
# Anti-Fraud Controls

- Anti-Fraud controls can be a powerful deterrent, as well as a proactive prevention and detection mechanism in the fight against fraud.
- Organization can benefit by knowing which anti-fraud controls are commonly used by their peers, as well as which tend to be most effective.



# Most Common Anti-Fraud Controls

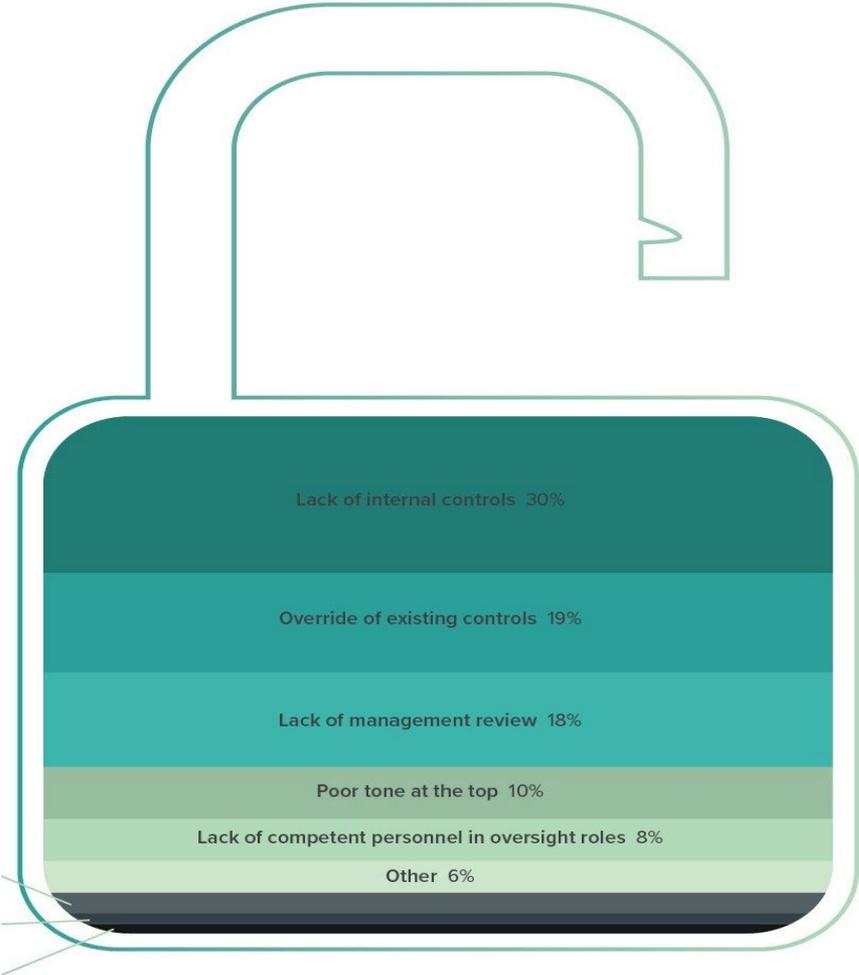
FIG. 17 What anti-fraud controls are most common?



# Anti-Fraud Controls Effect on Median Loss

Control	Percent of cases	Control in place	Control not in place	Percent reduction
Code of conduct	80%	\$ 110,000	\$250,000	56%
Proactive data monitoring/analysis	37%	\$ 80,000	\$ 165,000	52%
Surprise audits	37%	\$ 75,000	\$ 152,000	51%
External audit of internal controls over financial reporting	67%	\$100,000	\$200,000	50%
Management review	66%	\$100,000	\$200,000	50%
Hotline	63%	\$100,000	\$200,000	50%
Anti-fraud policy	54%	\$100,000	\$ 190,000	47%
Internal audit department	73%	\$108,000	\$200,000	46%
Management certification of financial statements	72%	\$109,000	\$ 192,000	43%
Fraud training for employees	53%	\$100,000	\$ 169,000	41%
Formal fraud risk assessments	41%	\$100,000	\$ 162,000	38%
Employee support programs	54%	\$100,000	\$ 160,000	38%
Fraud training for managers/executives	52%	\$100,000	\$ 153,000	35%
Dedicated fraud department, function, or team	41%	\$100,000	\$ 150,000	33%
External audit of financial statements	80%	\$120,000	\$ 170,000	29%
Job rotation/mandatory vacation	19%	\$100,000	\$ 130,000	23%
Independent audit committee	61%	\$120,000	\$ 150,000	20%
Rewards for whistleblowers	12%	\$ 110,000	\$ 125,000	12%

# Internal Control Weaknesses & Fraud



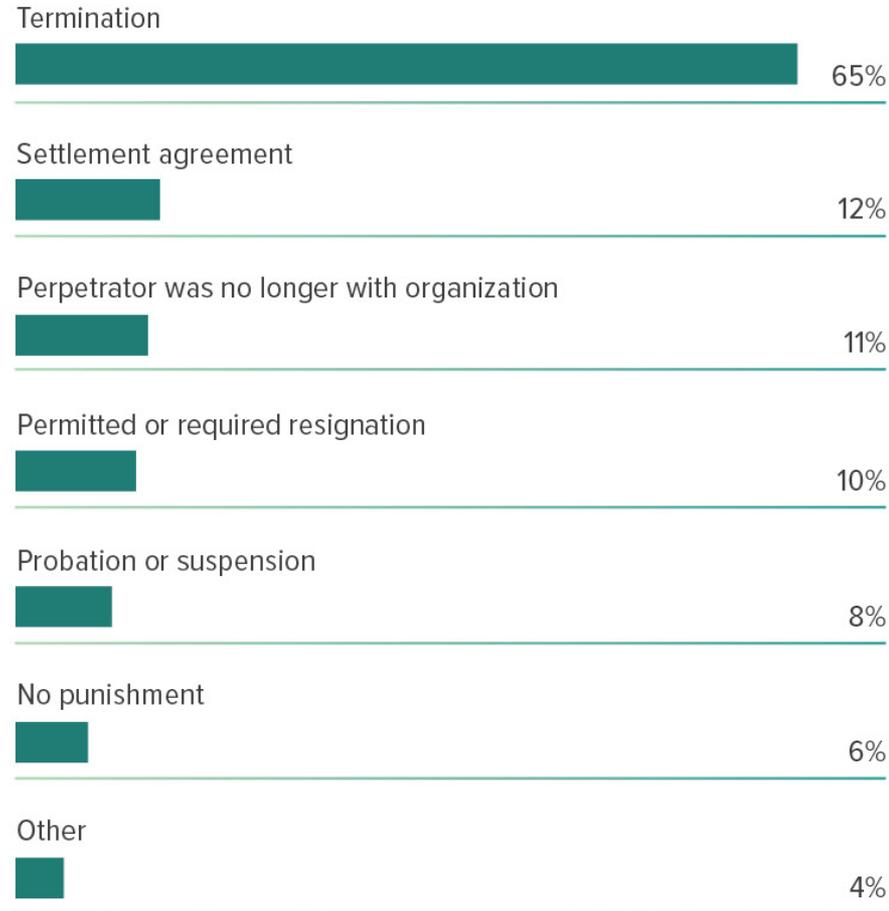
# Fraud Case Results



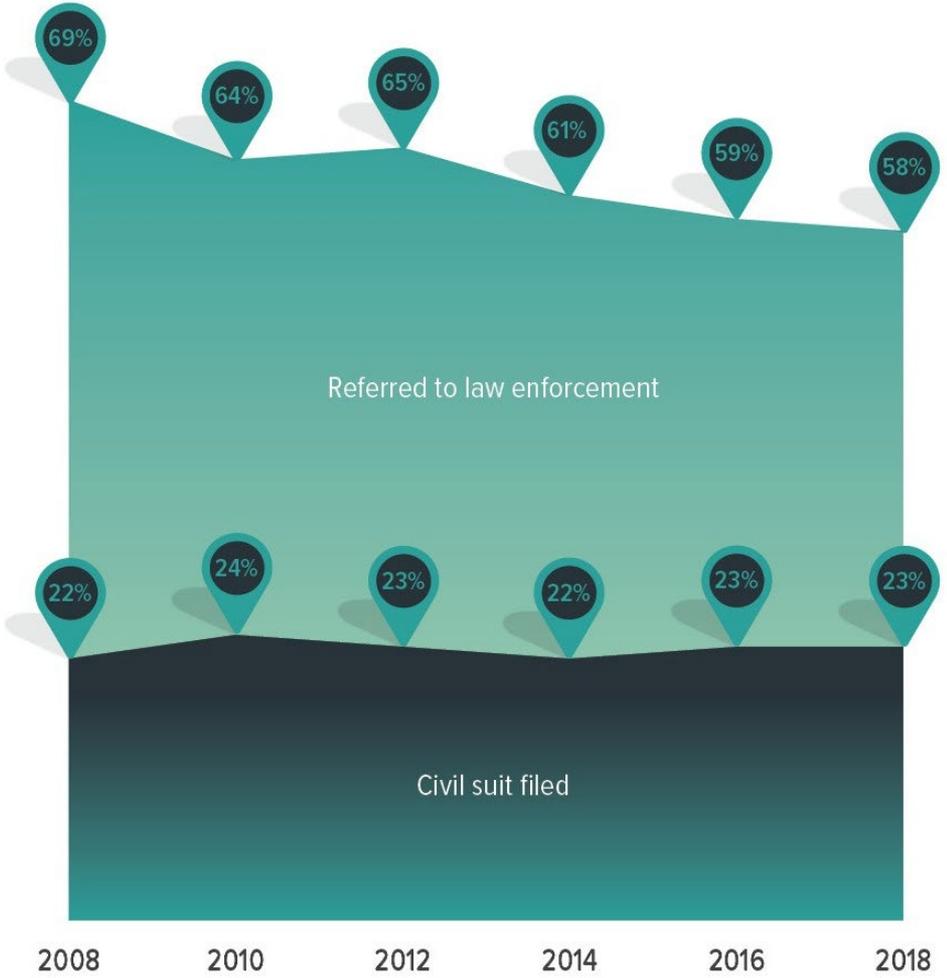
- How do organizations react after a fraud has been discovered?
- While it is often worthwhile to pursue remedial actions against perpetrators, victims will usually not be made whole.

# Internal Action Against Perpetrator

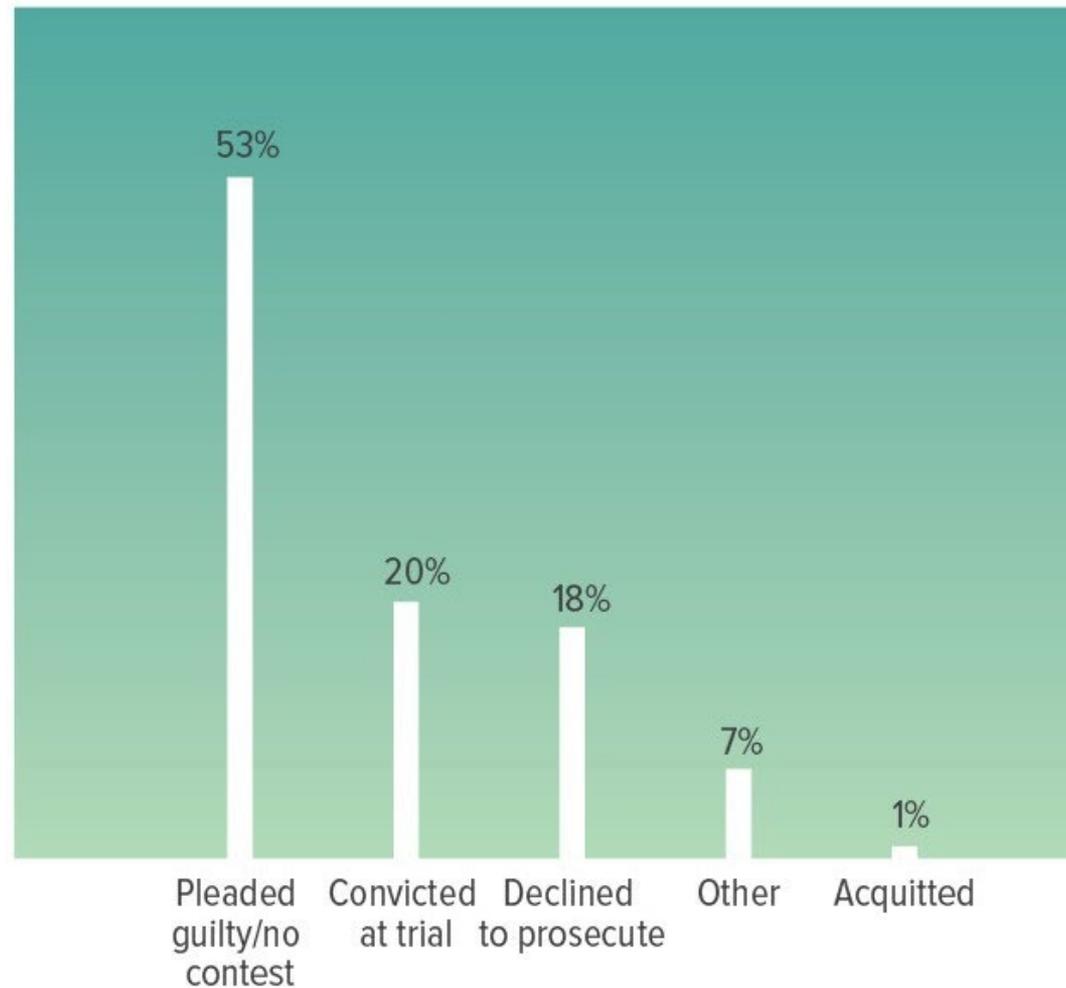
FIG. 41 How do victim organizations punish fraud perpetrators?



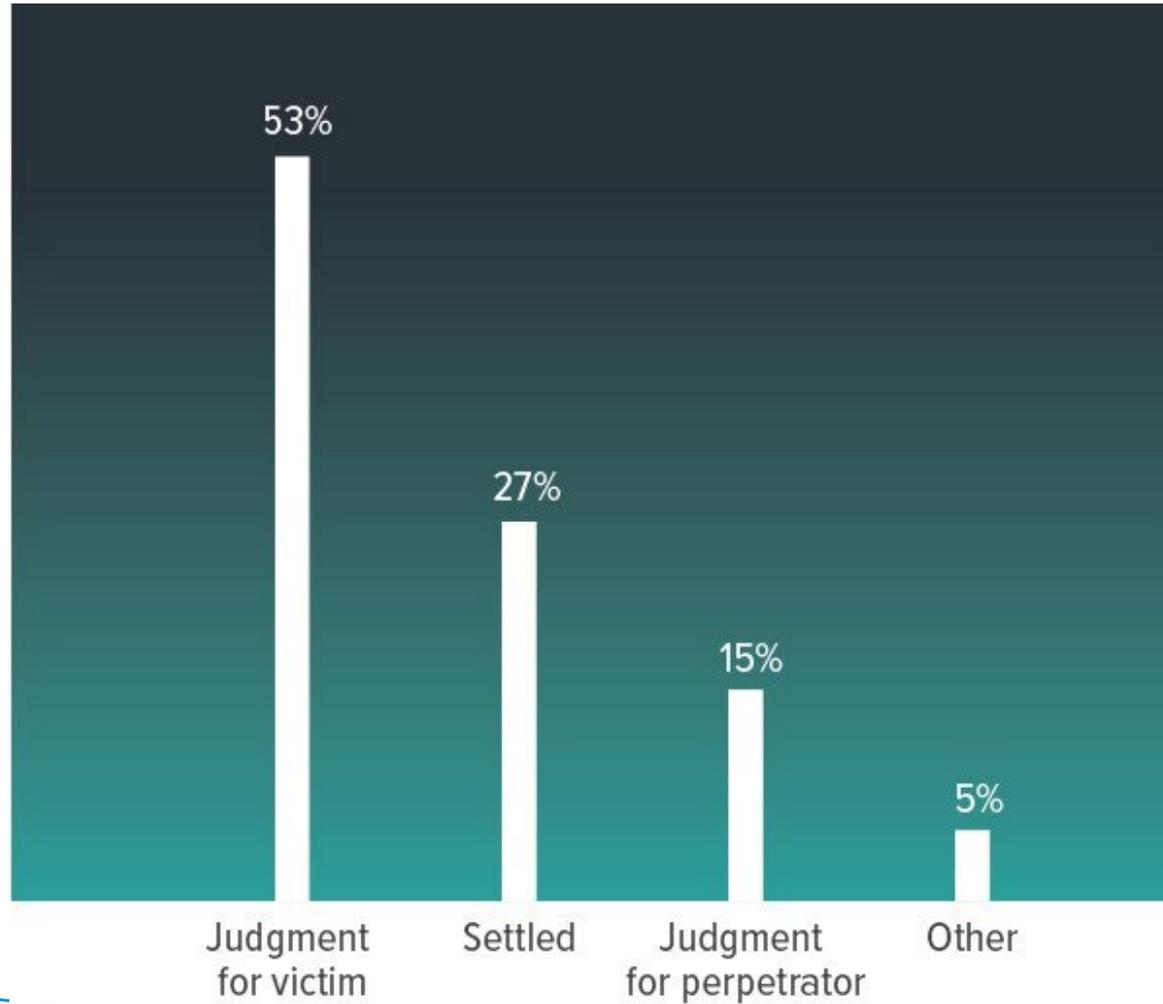
# Criminal Prosecutions & Civil Suits



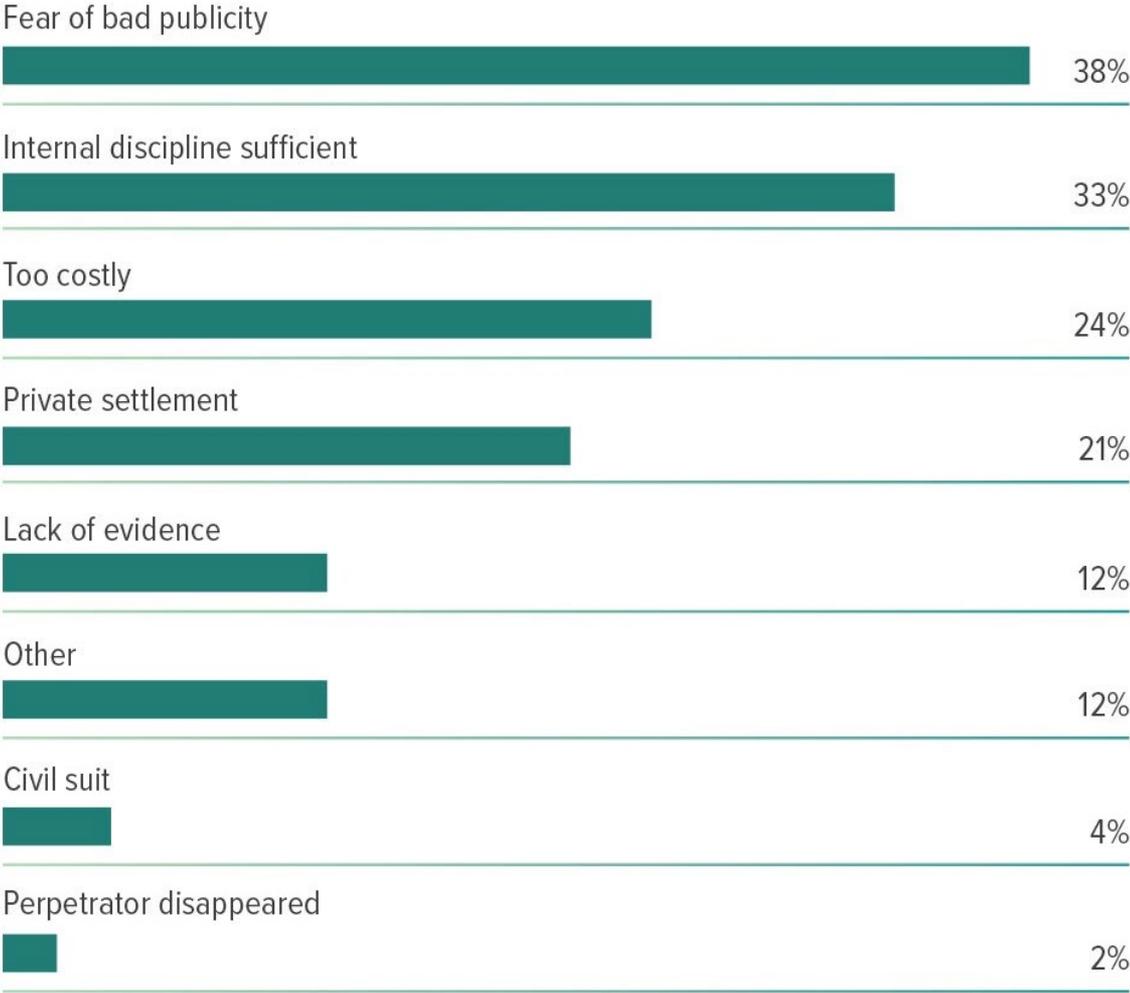
# Results of Criminal Referrals



# Results of Civil Suits



# Reasons for Not Referring to Law Enforcement



# Red Flags of Fraud

Conditions and symptoms that exist creating an increase in the risk of fraud.





# Red Flags of Fraud

- Environmental
- Internal Control
- Financial Statement
- Personal





# Environmental Red Flags

- Type of Management
- Poor Tone at the Top
- Financial Conditions at Company
- Opportunities for Advancement
- Political Environment





# Internal Control Red Flags

- Poor Segregation of Duties
- Weak Management Oversight
- No Job Descriptions
- Management Override
- Lack of Enforcement of Policies





# Financial Statement Red Flags

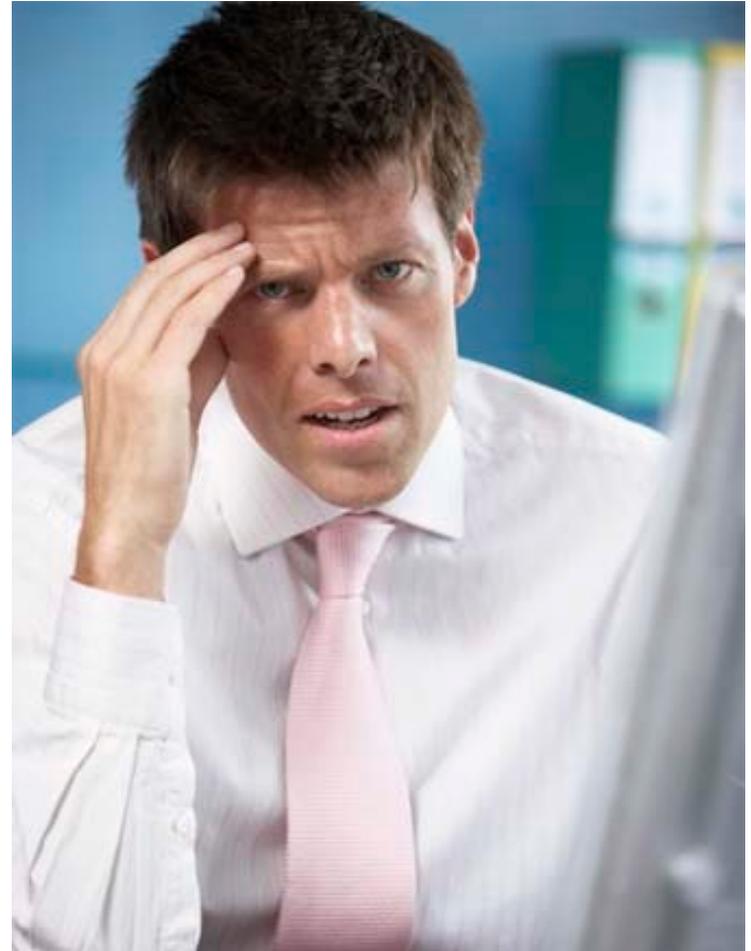


- Unexplained Changes in Revenue
- Changes in Gross Profit
- Changes in Expenses
- Inventory Shortages



# Personal Red Flags

- Financial
- Habits
- Feelings
- Others





# Financial Red Flags



## Need for Money

- Health Problems/Expenses
- Life Event
- Support of Ex-Spouse and Children
- Maintenance of Life Style



# Habit Red Flags

- Drugs
- Alcohol
- Gambling
- Investing (Day Trader)
- Life Style



# Feeling Red Flags



## Perception of Unfair Treatment By Employer

- Raise
- Promotion
- Perks
- Responsibility
- Discrimination

## Resentment of Supervisors

- Inappropriate Treatment
- Greater Competence Than Supervisor
- “Member of Family”

## Job Frustration

## Depression





# Other Red Flags

## Abruptly Changed Behavior

- Work Hours
- Resists taking vacation
- Displays of Wealth
- Attitude Toward Work/  
Coworkers
- Secrecy
- Possessiveness





# Purchasing Red Flags

- Payments sent to a P.O. Box
- No telephone number on invoice
- No street address on invoice
- Only one person is the contact with vendor
- Name of company has initials in it
- Similarity in initials to employee
- Invoices are for services and not materials





# Payroll Red Flags



- One person hires employees
- Same person has the ability to set up and remove employees in system
- Same person prepares/approves budget
- Employees do not sign time sheets
- Same person reviews/ approves total labor hours
- Multiple locations with no direct supervision



# Kickbacks Red Flags

- One person selects vendors
- Same person approves prices for equipment/materials/supplies
- No competitive bidding
- No independent review of prices/costs
- No company policy re: conflict of interest
- No company policy re: accepting of gifts



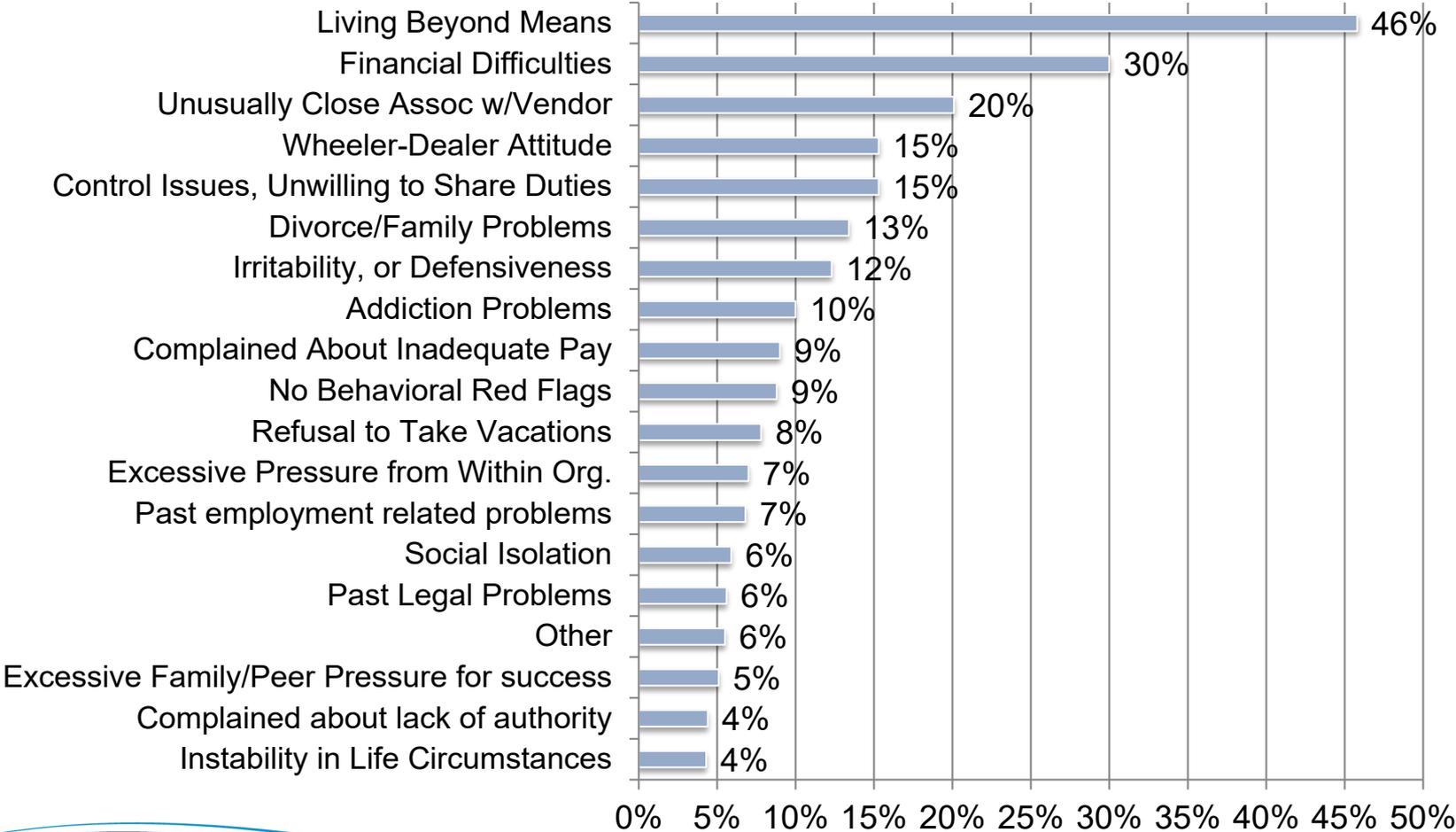


# Billing/Cash Receipts Red Flags

- One person prepares invoices and handles cash receipts
- Same person opens the mail
- Same person can write off a bad debt
- Same person handles customer complaints
- No review or supervision over invoicing
- Poor control over inventory



# Behavioral Red Flags During Fraud Scheme Asset Misappropriation



# Should You Focus on Prevention or Detection?

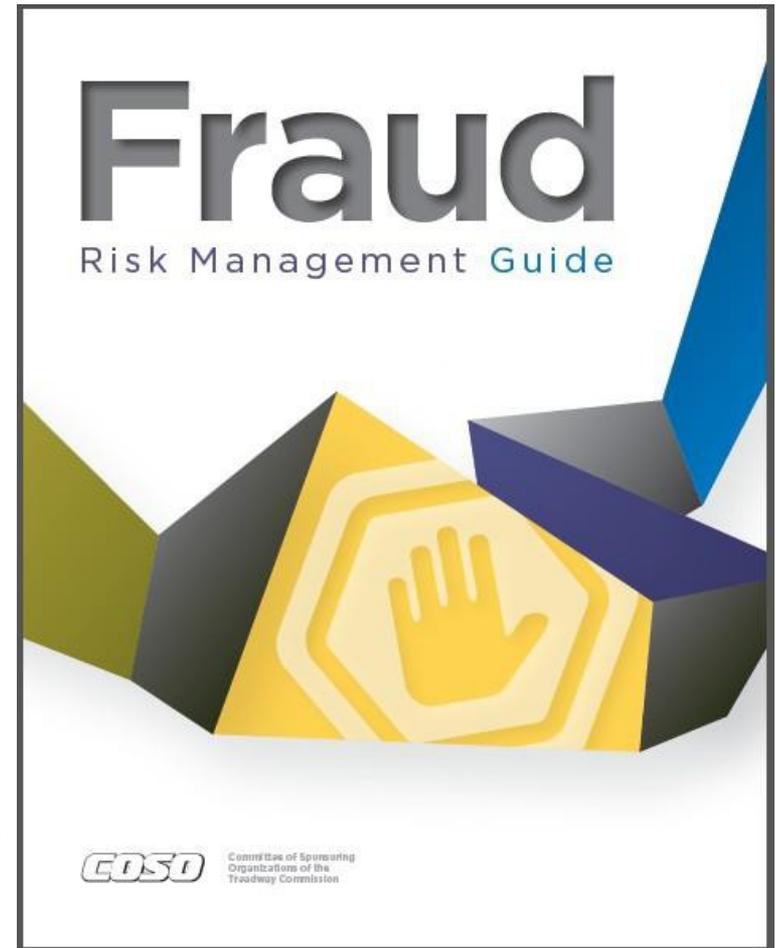
Answer: Both



- Take proactive steps to prevent
- Be skeptical, informed, and alert in order to detect as quickly as possible

# 2016 COSO Fraud Risk Management Guidelines

1. Establishment of a Fraud Risk Management Program
2. Perform comprehensive fraud risk assessments
3. Selects, develops & deploys preventative and detective fraud control activities
4. Investigation program and corrective actions
5. Ongoing evaluations & corrective action of the overall program



# Managing Fraud Risk

The COSO Fraud Risk Management Guide states:

*“The board of directors, and top management and personnel at all levels of the organization — including every level of management, staff, and internal auditors — have responsibility for managing fraud risk.”*

**"Fraud deterrence is achieved when the organization":**

- Establishes a visible and rigorous fraud governance process
- Creates a transparent and sound anti-fraud culture
- Includes a thorough fraud risk assessment periodically
- Designs, implements, and maintains preventive and detective fraud control processes and procedures
- Takes swift action in response to allegations of fraud, including, where appropriate, actions against those involved in wrongdoing

# Summary of Fraud Risk Management Components and Principles

---



Control Environment

**Principle 1** The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.



Risk Assessment

**Principle 2** The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.



Control Activities

**Principle 3** The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.



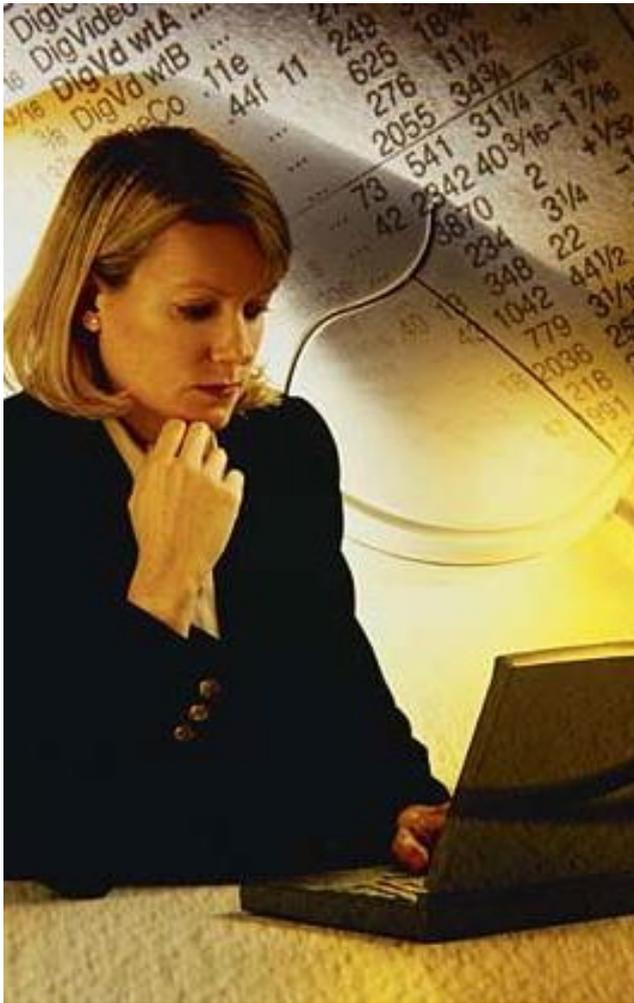
Information & Communication

**Principle 4** The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.



Monitoring Activities

**Principle 5** The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.



# Principle 1 - Fraud Risk Governance

# Principle 1 – Fraud Risk Governance

## Board and Senior Management:

- Makes an organizational commitment to fraud risk management.
- Supports fraud risk governance.
- Establishes a comprehensive fraud risk management policy.
- Establishes fraud governance roles and responsibilities throughout the organization.
- Documents the fraud risk management program.
- Communicates fraud risk management at all organization levels.

# Analytics considerations

## Principles 1 through 5: Aligned with Governance

Control Environment

### COSO 2013 Framework Principles

1. The organization demonstrates a commitment to integrity and ethical values

2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.



### Fraud Risk Management Principles

1. The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.



### Analytic Considerations

- Executive reporting
- Interactive dashboards
- Targeted analysis around metrics, compliance and ratios

# Principle 2 – Fraud Risk Assessment

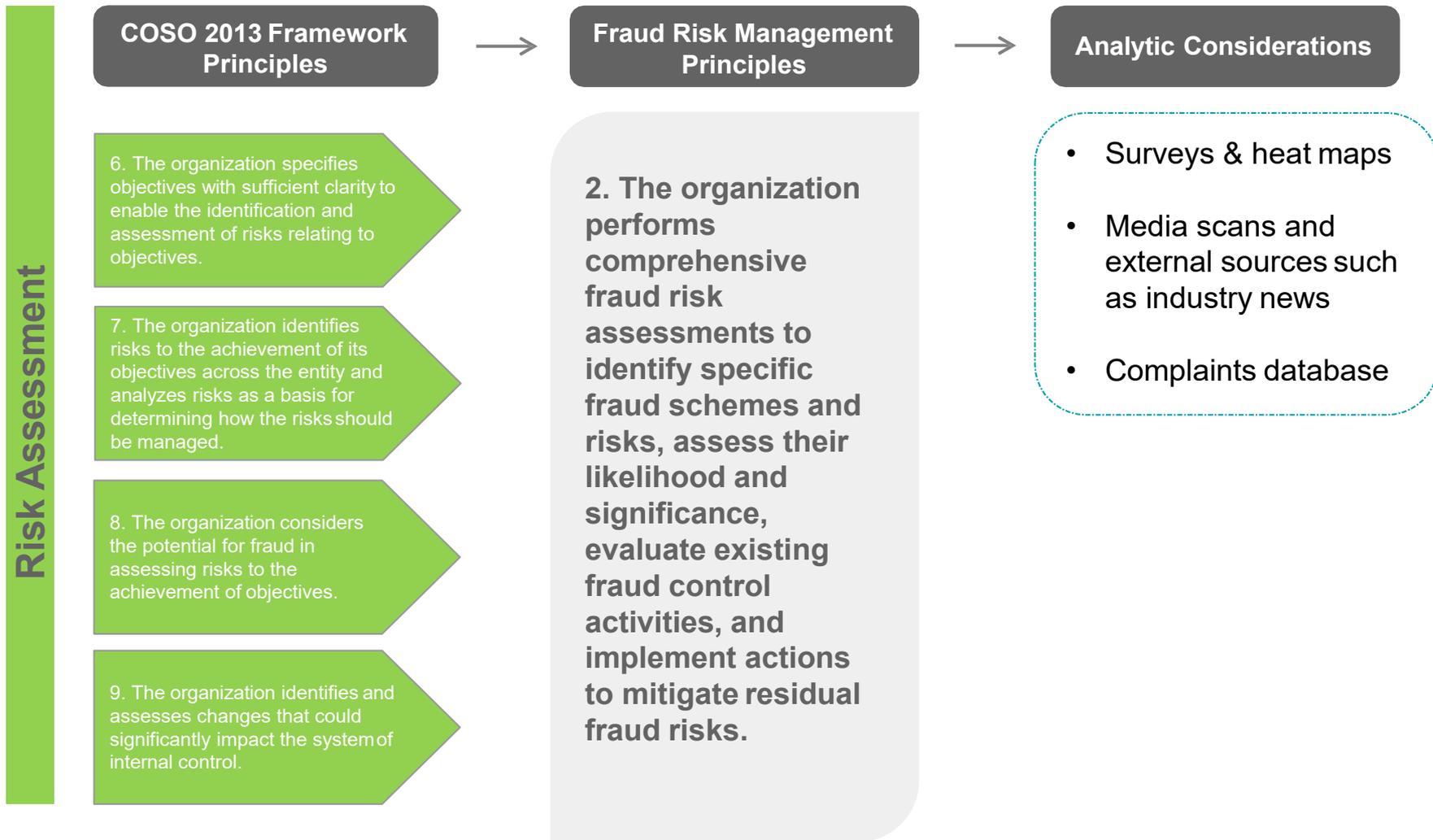


# Principle 2 – Fraud Risk Assessment

- ✓ Involves the appropriate level of management
- ✓ Analyzes internal and external factors
- ✓ Considers various types of fraud
- ✓ Specifically considers the risk of management override of controls
- ✓ Assess personnel or departments involved and all aspects of the fraud triangle
- ✓ Identifies existing fraud control activities and assesses their effectiveness
- ✓ Uses data analytics techniques for fraud risk assessment and fraud risk responses
- ✓ Performs periodic risk assessments and assess changes to fraud risk

# Analytics considerations

## Principles 6 through 9: Aligned with Fraud Risk Assessment



# Principle 3 - Fraud Control Activities

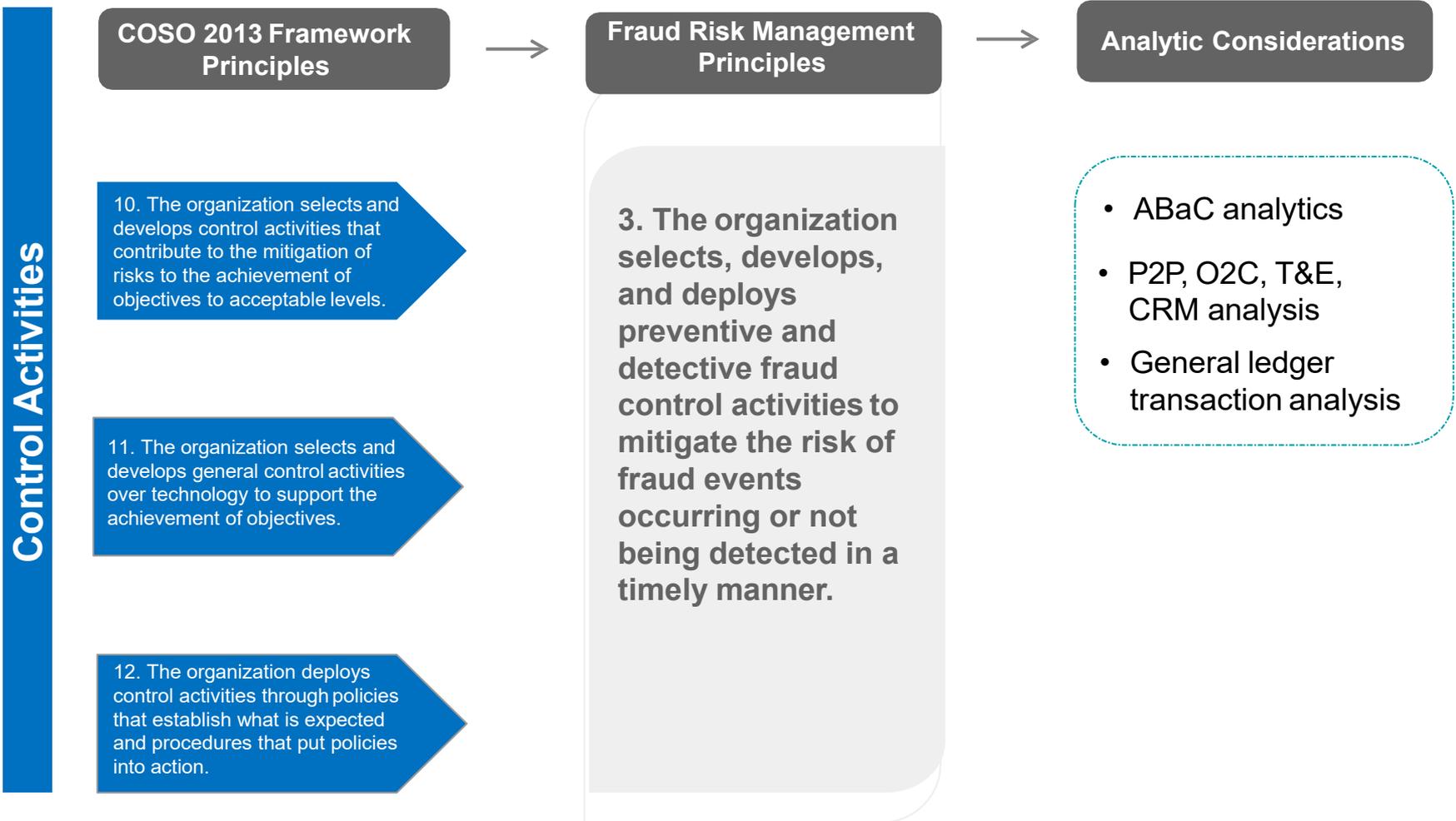


# Principle 3 – Fraud Control Activities

- Promotes fraud deterrence through preventive and detective control activities
- Considers organization-specific factors and relevant business processes
- Utilizes a combination of fraud control activities
- Considers management override of controls
- Utilizes proactive data analytics procedures
- Implements control activities through policies and procedures

# Analytics considerations

## Principles 10 through 12: Aligned with Fraud Control Activities



# Utilizing data analytics to do more

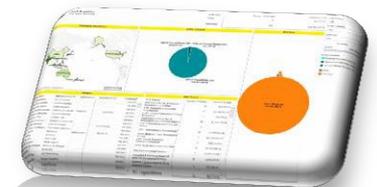
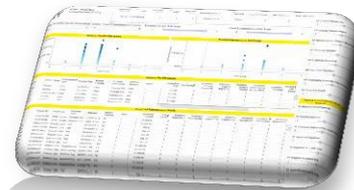
## Plan and build tests for:

- Payment risk scoring
- Vendor risk scoring
- High risk transactions
- Revenue recognition or sales commissions
- Conflicts of interests

## Additional tests for enhanced reviews:

- ✓ Inventory management
- ✓ Salaries & payroll
- ✓ Employee travel & entertainment
- ✓ FCPA/UKBA (corruption risks)

# Principle 4 - Fraud Investigation and Corrective Action



# Principle 4 - Fraud Investigation and Corrective Action

- Establishes fraud investigation and response protocols
  - Confidentiality, urgency, evidence preservation, legal protections, forensic support, investigation protocols, reporting process, root cause and mitigating controls, etc.
- Conducts investigations
- Communicates investigation results
- Takes corrective action
- Evaluates investigation performance

# Why a formal investigation program is necessary?

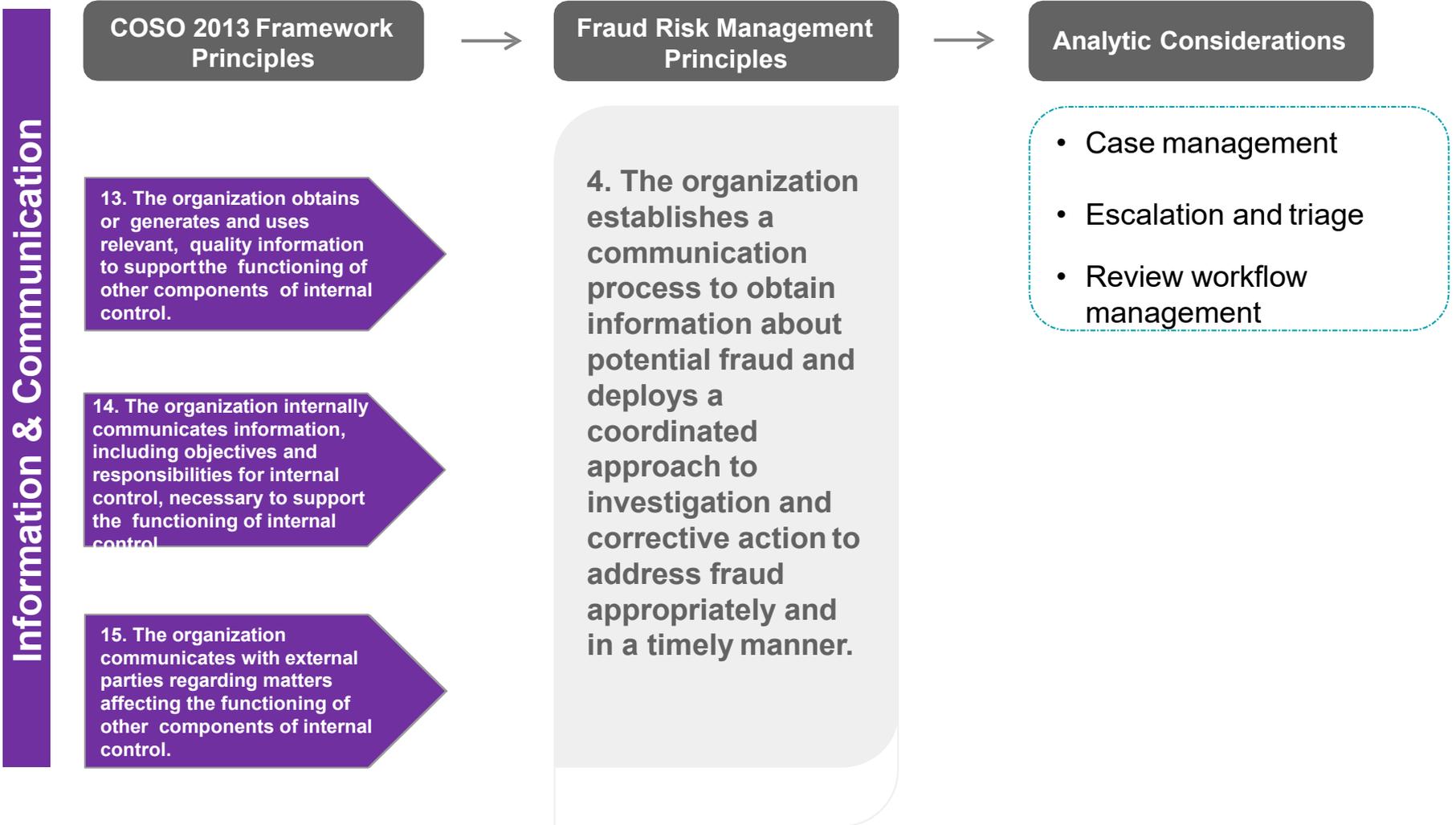
- Poorly performed investigations
- Key source of problems not obtained and internal controls not improved,
- Lack of dedicated and experienced forensic or investigative skill sets,
- Lack of routine and repetitive investigation training
- Development of corrective action plan and monitoring activities not consistently applies

# Monitoring investigation performance

- Resolution time and investigation costs
- Repeat incidents
- Value of losses recovered and future losses prevented
- Corrective actions
  - ✓ Internal control remediation, business process remediation, disciplinary action, training, insurance claims, extended investigations, civil actions, criminal referrals
  - ✓ \*\*Corrective actions for fraud related incidents is an evaluation component within the Federal Sentencing Guidelines

# Analytics considerations

## Principles 13 through 15: Aligned with Investigative Activities



# Principle 5 - Fraud Risk Management Monitoring Activities

EY Counter Fraud Management

Risk Ranking | Tasks | Alerts | Global Reporting Dashboard | Add Trader Review

**Profile**  

**John Smith**  
 Fx\_Dealing  
 Sao Paulo

**Risk elements**

Category	Employee Score	Desk Average	View associated files
Trade Analytics	5.5	6.0	Here
Voice Log Activity	4.0	3.2	Here
Travel Activity	5.3	4.1	N/A
Email Activity	9.3	6.2	Here
Chat Activity	2.0	0.5	Here

**Recent alerts & Investigations**

ID	Date	Type	Risk	Disposition
2323.12	3/2/2015	Ethics	Low	Closed
5424.32	3/31/2015	Unauthorized behavior	Low	Closed
1232.12	5/2/2015	Unauthorized behavior	Low	Closed

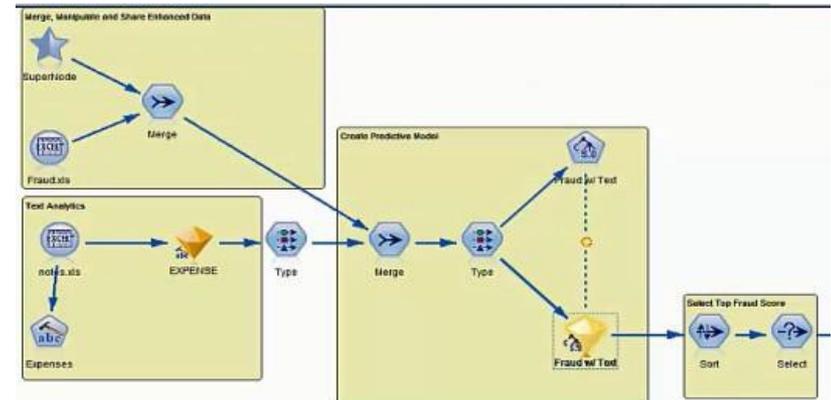
**Initiate review**

Status: Not Started  
 Issue Type:  
 Include peers:  
 Start Date: 10/13/2015  
 End Date: 10/13/2015  
 Assign Analyst:

**Ontologies referenced**

- US trade surveillance ontology\_v2.3
- Portuguese trade surveillance ontology\_v1.4
- Global trade manipulation ontology\_v3.5

Initiate Investigation | Cancel



# Principle 5 - Fraud Risk Management Monitoring Activities

- ❖ Considers a mix of ongoing and separate evaluations
- ❖ Considers factors for setting the scope and frequency of evaluations
- ❖ Establishes appropriate measurement criteria
- ❖ Considers known fraud schemes and new fraud cases
- ❖ Evaluate, communicates and remediates deficiencies

# What should organizations do now?

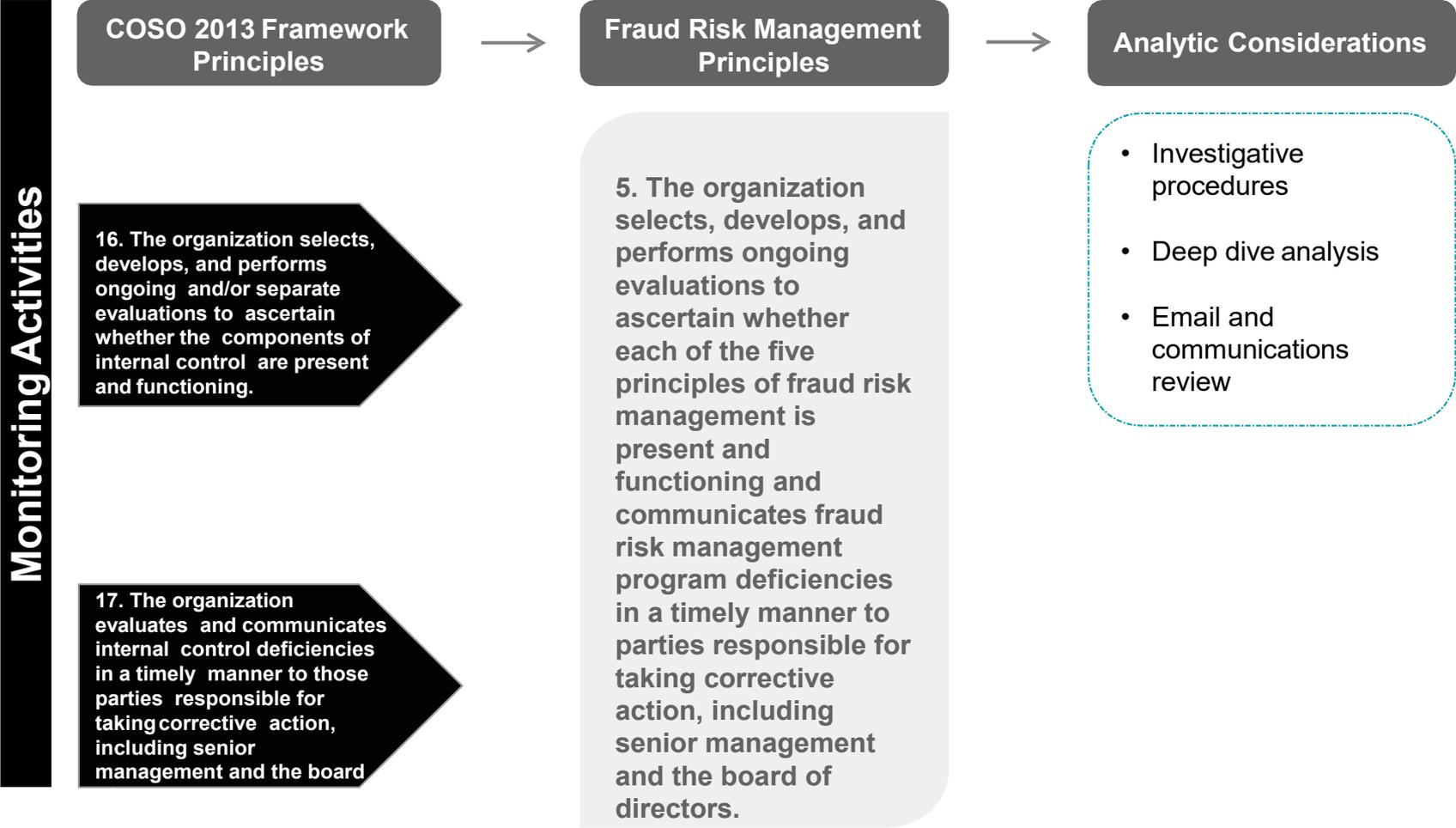
The COSO Anti-Fraud Guide sets out a process for on-going, comprehensive fraud management.

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process



# Analytics considerations

## Principles 16 & 17: Aligned with Monitoring Activities

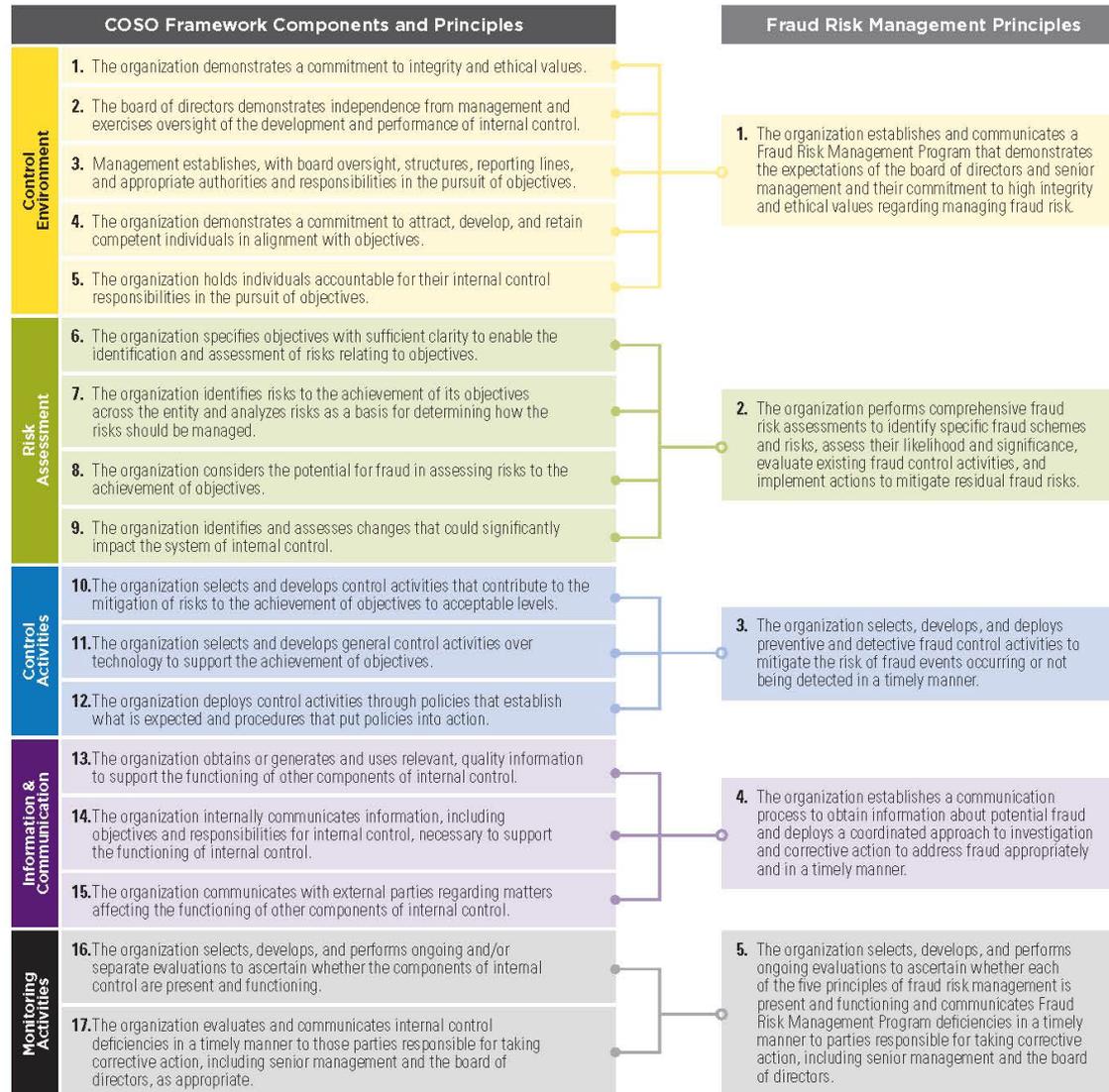


# Key takeaways and next steps

- Identify and assign the appropriate Process Owner/Champion within your organization
- Determine the appropriate level of adherence to COSO ERM Framework, whether formal, informal or not at all
- Identify and formalize all anti-fraud and investigation activities within the fraud risk management program
- Conduct an assessment to identify gaps, weaknesses and duplicative or ineffective anti-fraud efforts
- Develop, document and Implement comprehensive preventative and detective data analytics functions

# Relationship Between the 2013 COSO Framework's Five Components and 17 Internal Control Principles and this Guide's Five Fraud Risk Management Principles

COSO revised its 1992 *Internal Control — Integrated Framework* in 2013 to incorporate 17 principles. These 17 principles are associated with the five internal control components COSO established in 1992. This guide's five fraud risk management principles fully support, are entirely consistent with, and parallel the 2013 COSO Framework's 17 internal control principles.<sup>7</sup> The correlation between the fraud risk management principles and the 2013 COSO Framework's internal control components and principles is as follows:



# Case Studies

- Description of fraud claim
- Assess risks
- Discuss forensic procedures
- Discuss results
- Discuss controls that could have mitigated fraud
- Discuss improvements for future frauds

# Case Study #1

## County Government

- Case setup
  - Large department within County Government
  - Issues surrounding the entry of time and PTO in Time and Attendance system
  - Allegations included the following:
    - Employees were sharing login and passwords (to the time and attendance application) with each other, logging in and/or out for each other prior to late arrival or after early departure
    - Supervisory employees were manually overwriting punch in/out transactions (i.e. times of punch in transactions)
  - Assess the risks

# Case Study #1

## County Government

What type of forensic procedures would you utilize at the County Department in attempts to confirm or deny the allegations?

What order would you do them in?

Why is that important?



# Case Study #1

## County Government

- Forensic Procedures
  - Interviews – Director, Supervisors, Time & Attendance ( T&A) Admins, all other staff
  - Gain an understanding of each individual's access rights, and user rights within the T&A system
  - Work with County IT department to export data from the T&A system to list daily log In/Out times during the scope period for each employee
  - Work with County IT Department to identify individual IP Addresses and County Network login In/Out times during the scope period for each employee

# Case Study #1

## County Government

- Forensic Procedures – What did we do?
  - Reconciled the Log In/Out times in the T&A system to the Log In/Out times in the County Network to identify instances where there were material differences
  - Interview the individual employees to discuss possible reason for material differences
  - Aggregated the total time differences over the scope period to identify the total time that was fraudulently reported for each individual

# Case Study #1

## County Government

- Results

- Several individual employees were fraudulently reporting their time over multiple years
- Several employees were colluding to do so, and then colluding to cover up their schemes
- Employees had a rotation whereby they would take turns leaving early or arriving late and have another employee log them in/out

# Case Study #2

## Local Government

- Case setup
  - Law Enforcement Agency
  - Allegations involved the following:
    - Officers were submitting manual OT slips for time that they did not work
    - Officers were submitting OT vouchers for Court appearances occurring on the same day, as separate court appearances on multiple days. Each instance was guarantee for 4 hours.
  - Assess risks

# Case Study #2

## Local Government

What type of forensic procedures would you utilize for the Law Enforcement Agency?

What order would you do them in?

Why is that important?



# Case Study #2

## Local Government

- Forensic Procedures

- Interviews – Captain/Chief, officers, administrative employees, HR representatives
- Determine who is responsible for the timekeeping within the Agency
- Determine what the scope period is?
- Gain an understanding of the T&A package, the manual process utilized, and the internal controls in place etc.
- What information is available to support hours worked?
- Gather all applicable information

# Case Study #2

## Local Government

- Forensic Procedures – What did we do?
  - Interviews – Learned that separate Payroll rep's were housed within the Local Government and the Law Enforcement Agency
    - Each process was extremely manual with multiple spreadsheets and several manual adjustments needed each pay period
  - Learned that no time limit on how long after OT was worked that an employee was required to submit OT voucher
  - Discovered that the Director/Chief was not monitoring the OT vouchers closely, nor reconciling the vouchers submitted for past pay periods

# Case Study #2

## Local Government

- Forensic Procedures – What did we do?
  - Examined every OT voucher submitted during the scope period, confirmed appropriate approval, mathematical accuracy, and specific circumstances we could verify
  - Learned that nobody was reconciling the OT vouchers submitted for Court Appearances to the actual Court Dockets to ensure employees actually had a court case.
  - We worked with Director/Chief to locate any other transactions journals or available reports to confirm individual officer’s activity “on the job” during the OT hours submitted
    - Arrest reports, traffic tickets written, training attended, etc.

# Case Study #2

## Local Government

- Results

- Officers were indeed separating court appearances that occurred during same morning session, into separate OT vouchers occurring on different days. Each instance was contractually guaranteed for a minimum of 4 hours of OT.
- Officers submitted OT vouchers, and were subsequently paid for time that was never actually worked
- No Chief/Director oversight led to disciplinary action
- Individual Officers were disciplined and/or terminated

# Case Study #3

## Local Government

- Case setup
  - Town Government
  - Board members had concerns about Clerk and cash procedures within the operations
  - Clerk had access to, and control over all finances
  - Clerk had health problems causing financial strains
  - Clerk processed several cash transactions for the Town such as permits and vital records etc.
  - Town operated landfill was cash basis operation and there were concerns with the individual responsible for the operations

# Case Study #3

## Local Government

What type of forensic procedures would you utilize at the Town to confirm/refute allegations?

What order would you do them in?

Why is that important?



# Case Study #3

## Local Government

- Forensic Procedures
  - Interviews – Town Board Members, Town clerical staff, Town Clerk
  - Gather information about processes
    - Cash controls at the Town Office as well as the Landfill
    - Bank accounts
    - Use of petty cash
  - Obtain bank statements for the scope period, including cancelled checks, bank reconciliations etc.

# Case Study #3

## Local Government

- Forensic Procedures – What did we do?
  - Conducted Interviews – Learned what type of control the Clerk had over the cash processes as well as the bank accounts
  - Interviewed the Landfill Operator to learn of his processes – found that virtually no controls were in place to reconcile cash received
  - Interviewed the Board members to gather additional information relative to additional allegations and/or concerns
  - Reconciled the manual transaction logs utilized for the vital records transactions to the actual cash receipts for reasonableness
  - Inspected the transactions in the bank accounts in search of any transactions appearing to be inappropriate, suspicious, or for personal purchases
  - Reviewed the journal entries booked by the Clerk for appropriateness, and investigated where necessary

# Case Study #3

## Local Government

- Results

- Clerk was pocketing most of the cash received to process vital records and/or permits etc.
- Clerk was colluding with the Landfill Operator to steal large sums of cash from the Landfill
- Clerk was spending thousands of dollars on personal on-line shopping and a Town office was full of packages
- Third party Accountant was not performing any due diligence, rather just booking transactions as they were told

# Case Study Take-Aways

## Be Aware of the Risks / Be Proactive / Professional Skepticism

- Don't allow employees to be put in a position where fraud is even possible – protect your employees as much as you protect your organization
- Analyze Risk – Continually as:
  - Systems change
  - Business activity changes
  - Positions change – downsizing
- Segregate duties – use board members, other departments and regular internal audits to protect risky transactions
- Establish Open Door and Whistleblowing Policy

Thank you for your  
attention.



Questions?