

OAPT Conference Understanding Internal Control & Fraud Prevention June 12, 2018

Presented by:
Derek Conrad, CPA
Senior Manager, Government Services
Jennifer Masters, CPA
Manager, Government Services



Agenda

- Five Components of Internal Control
- Fraud Triangle
- Fraud Risk Assessment
- Fraud Statistics
- Fraud Prevention Tips

What is the definition of Internal Control?

- Internal Control can be defined as the sum of:
 - An accounting procedure or system designed to promote :
 - Efficiency and effectiveness
 - Ensure the implementation of a policy
 - Safeguard of assets
 - Reduce risk of fraud
 - Minimize errors

Five components of Internal Control

- Control Environment
- Risk Assessment
- Information and Communication
- Control Activities
- Monitoring

Internal Control – Control Environment

- **Definition** – Management’s attitudes, awareness, and actions concerning the importance of a control.
 - The Environment sets the “tone” of the entity
 - Influences the control consciousness of it’s people
 - Serves as the foundation for all internal control components, providing components, discipline, and structure.
- The best *designed* policies and procedures have little hope of being effective without the proper “tone at the top”.
 - Management must lead by example. Controls are not limited to staff.

Internal Control – Risk Assessment

- **Definition** – The entity’s identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risk should be managed.
 - This is an *ongoing* process. The risks of yesterday may not be the risks of today or tomorrow.
 - Risks must not only be identified, but must be *anticipated* so they can be avoided or mitigated. (analogy – installation of lights at a railway crossing *before* an accident occurs).
 - Managements focus on *identifying risk* should start with change:
 - Change in operating environment
 - Change in personnel
 - Change in information systems and technology
 - New programs or services provided
 - Change in structure

Internal Control – Risk Assessment con’t

- Management should also focus on the *inherent risks*
 - Complexity
 - Cash receipts
 - Third-party beneficiaries
 - Prior problems
 - Prior unresponsiveness to identified control weaknesses
 - Payroll withholdings
 - Fake vendors
 - Credit/purchase cards
 - Central garage/storage locations
- Proper training, ongoing efforts, responsiveness and commitment to ongoing assessment will strengthen internal controls to ensure a strong framework.

Internal Control – Information & Communication

- **Definition** – The identification, capturing, and exchange of information in a form and on a timely basis to enable employees to carry out their responsibilities.
 - Management must be able to obtain reliable information to determine and assess risk and communicate policies and other information to those who need it.
 - Potential issues effected by *information*:
 - The entity’s performance evaluation vs strategy or goal
 - Impact on efficiency and effectiveness
 - Management decisions on use of resources (financial or human)
 - Management can develop the best internal control environment, policies and procedures, etc., however if not properly *communicated* they may as well not exist.
 - Written policies and procedures distributed
 - Training programs established
 - New hire orientations
 - Policies posted on websites for easy access

Internal Control – Information & Communication con't

- Potential issues facing *communication* of information:
 - Effectiveness and efficiency in the performance of the duties of employees
 - Lack of communication channels available to employees to report suspected improprieties
 - Lack of timeliness making information less useful in decision making



Internal Control – Control Activities

📌 **Definition** – The policies and procedures that help ensure management directives are carried out.

→ As a result of ongoing *risk assessment* and the strategies to *communicate information*, management must develop policies and procedures to carry out and meet the goals and strategies of the entity.

→ Traditionally, control-related policies and procedures related to finance are classified into one of the following categories:

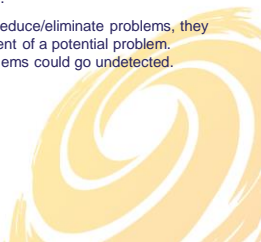
- Authorization
- Properly designed records
- Security/safeguarding of assets and records
- Segregation of duties
- Periodic reconciliations
- Analytical review



Internal Controls – Monitoring

📌 **Definition** – The process used by those charged with governance (management AND the elected taxing authority) to assess the quality of internal control over time.

- The best developed control policies and procedures require changes over time as the environment changes.
- Not only are controls implemented to reduce/eliminate problems, they should be designed to alert management of a potential problem. Without proper monitoring, these problems could go undetected.



Internal Controls – Monitoring con't

📌 The Roles in *monitoring* internal controls

→ Who is "ultimately" responsible for internal control?

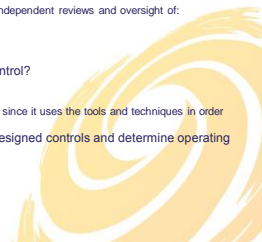
- THE GOVERNING BODY
 - It's the job of the governing board to ensure that management meets all of it's responsibilities.
 - How can this be achieved? Establish an "audit committee"
- Audit Committee responsibilities may include independent reviews and oversight of:
 - Reporting processes
 - Internal controls
 - Independent auditors

→ Who is "primarily" responsible for internal control?

- MANAGEMENT
 - Fundamentally a management concern since it uses the tools and techniques in order to achieve managements objectives

→ Who's role is it to "validate" the success of designed controls and determine operating effectiveness.

- YOUR AUDITORS



Internal Controls – Inherent Limitations

- 🔑 No internal control framework can be perfect.
- 🔑 Inherent limitations include:
 - Management over-ride of controls (policies and procedures)
 - Collusion
 - Cost of the control (policy or procedure) should not cost more than the benefit it is expected to achieve
 - Human judgment can be faulty, human errors and mistakes
 - Limitation on segregation of duties based on number of employees

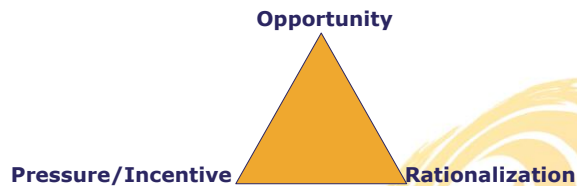
Internal Controls - Examples

- 🔑 Disbursements
 - Written approval of authorization to purchase
 - Review of account coding by knowledgeable employee
 - Written receipt of goods/services (okay to pay)
- 🔑 Payroll
 - Process for hiring/termination of employees
 - Review of account coding by knowledgeable employee
 - Approval of timecards
 - Approval of pay rates

Internal Controls - Examples

- 🔑 Receipts
 - Finance office receiving adequate support
 - Segregation of duties
 - Trend analysis
- 🔑 Manual Journal Entries (Memo/Correcting Entries)
 - Segregation of duties
 - Formal approval by management
 - Treasurer, Council/Board

Cressey's Fraud Triangle – Concept that dates back over half a century. Generally for fraud to occur, three things must be present:



Source: ACFE 2012 Report to the Nations on Occupational Fraud and Abuse

Fraud Triangle

- ④ **Pressure** – Financial need that is often unwilling to be shared (addictions, debt, etc.) or that emotions have impacted the person (sick child or “keeping up with the Joneses”)
- ④ **Opportunity** – The ability to commit a fraudulent activity must exist (weaknesses in internal control or the ability to override them)
- ④ **Rationalization** – When a person has the ability to justify their actions (I’m underpaid, I’ll pay it back, or the health of my child is more important)

Fraud Diamond



David T. Wolfe and Dana R. Hermanson

Capability

- ④ Individual traits and characteristics
 - Having the right organizational position or function to take advantage of fraud opportunities.
 - Having the appropriate expertise to take advantage of fraud opportunities.
 - Having the confidence or ego to take advantage of fraud opportunities.
 - Being able to coerce others to participate in fraudulent activities.
 - Being able to deal with the stress associated with committing fraud.
 - Being a good liar.

Fraud Pentagon



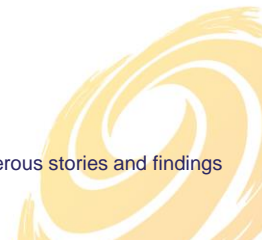
Competence & Arrogance

- 🔑 Competence – similar to capability in fraud diamond
- 🔑 Arrogance – Strong ego, attitude of superiority, entitlement and/or greed to commit fraud.



It Could Happen to You

- 🔑 Skimming of Cash Collections
- 🔑 Missing Evidence
- 🔑 IT Equipment and Purchases
- 🔑 Off-the Books Bank Accounts
- 🔑 Visit the AOS website for numerous stories and findings



What is Fraud Risk Assessment?

- 🔑 Proactive approach to mitigating fraud in your organization
- 🔑 Analyzing where fraud can occur in your organization
- 🔑 Fraud Prevention vs. Fraud Detection
 - Prevention = Proactive
 - Detection = Reactive



Who is Responsible for Risk Assessment

- 🔑 Governing Body
 - Audit or Finance Committee
- 🔑 Mayor/Administrator
- 🔑 Finance Director/Treasurer
- 🔑 Executive Staff
- 🔑 Everyone throughout the Organization– informal lines of communication



Definition of Fraud

- 🔗 "Intentional perversion of truth in order to induce another to part with something of value or to surrender legal right." (Mirriam-Webster's online dictionary)
- 🔗 Association of Certified Fraud Examiners (ACFE)
 - Misrepresentation of material facts
 - Concealment of material facts
 - Bribery
 - Conflicts of Interest
 - Theft of money and property
 - Breach of Fiduciary Duty



Risk Assessment Includes:

- 🔗 Risk Identification
- 🔗 Risk Likelihood
- 🔗 Significance Assessment
- 🔗 Risk Response



Risk Identification

- 🔗 Risk Identification
 - Gathering information from both internal and external sources
 - **Brainstorming**
 - Interviews
 - Outside training
 - Analytical Procedures
 - Trend analysis: vendor example
 - Monthly financial reports (budget vs actual, etc.)
 - Where are the inherent risks?
 - Cash collection points
 - Lack of oversight



Risk Identification cont.

- 🔗 Risk Identification
 - Incentives/Pressures
 - Budget constraints
 - Performance Bonuses
 - Opportunities
 - Cash collection points
 - Segregated accounts
 - Access to create vendors



Risk Likelihood

- 📌 Risk Likelihood
 - Financial exposure
 - Public opinion
 - Designed controls vs. Inherent risks
 - Is there a gap?

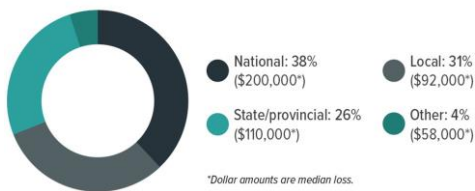


Risk Response

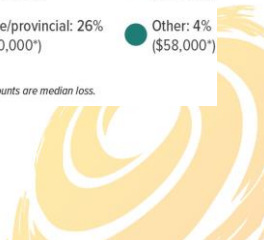
- 📌 Consider cost-benefit
 - Cost of Inaction
- 📌 How will council/management respond
 - Increased Training
 - Surprise Audits
 - Change in Policy and Procedure



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

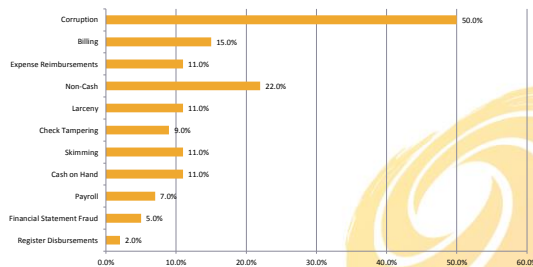


Source: ACE 2018 Report to the Nations on Occupational Fraud and Abuse

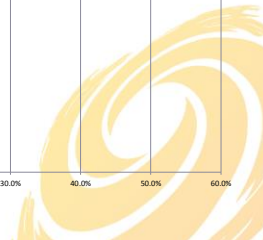


Types of cases at risk

Government and Public Administration
% of Cases

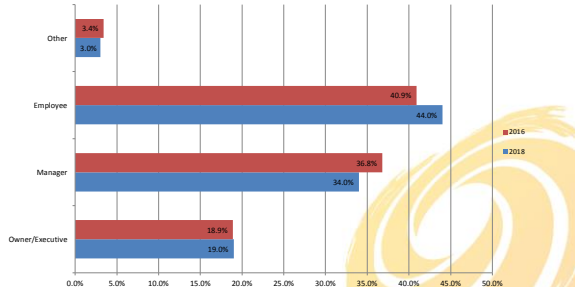


Source: ACE 2018 Report to the Nations on Occupational Fraud and Abuse



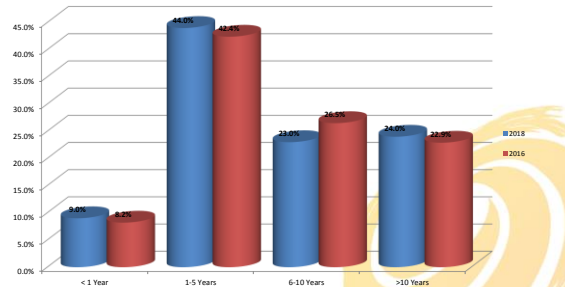
Who are the perpetrators?

Position of Perpetrator-Frequency



Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

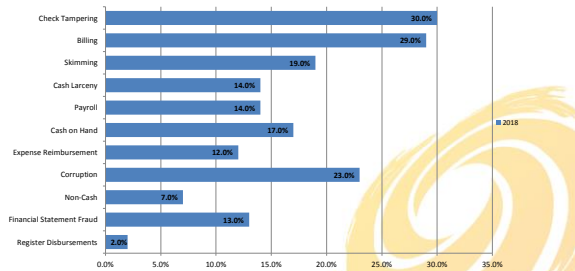
Tenure of Perpetrator



Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

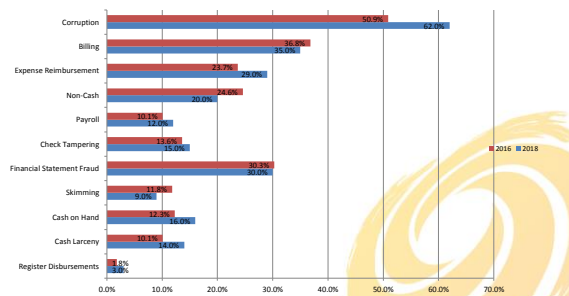
Schemes from Perpetrators working in Accounting Department

Accounting



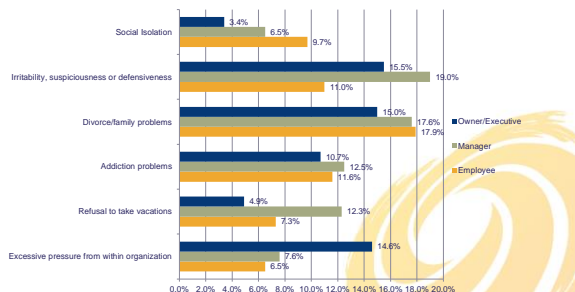
Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

Schemes from Perpetrators in Executive or Upper Management



Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

Behavioral Red Flags Based on Perpetrator's Position



Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

Behavioral Red Flags

Behavioral Red Flag	Percent of Cases
Living beyond means	41%
Financial Difficulties	29%
Unusually close association with vendor/customer	20%
Control Issues, Unwillingness to Share Duties	15%
Divorce/Family Problems	14%
Wheeler-Dealer Attitude	13%
Irritability, Suspiciousness or Defensiveness	12%

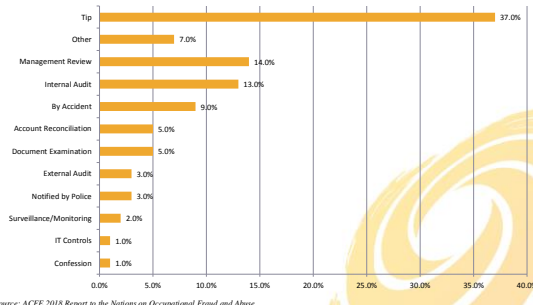
Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

Behavioral Red Flags

Behavioral Red Flag	Percent of Cases
Addiction problems	10%
Complaining about inadequate pay	9%
Excessive pressure from within company	7%
Social Isolation	7%
Past employment-related problems	6%
Past Legal Problems	6%

Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

Detection in US



Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

Billing Schemes

- 🔗 False invoicing through a shell company
- 🔗 Personal purchases with government funds
- 🔗 False invoicing through an established vendor



False Invoicing

- 🔗 Fake invoice – no service or product exchange
- 🔗 www.customreceipt.com



Fake invoices many times lack information

- 🔗 Street address – PO box only
- 🔗 Phone number
- 🔗 Good description
- 🔗 Logo
- 🔗 Packing slip for products purchased
- 🔗 Shipping destination for products
- 🔗 Invoice numbers are sequential



Vendor Files

- 🔗 What needs done to vendor's files
 - Clean vendor file annually
 - Vendor approval process
 - Training
 - Google new vendor requests
 - IT controls limiting access



Employee Expense Reimbursements – What to look for:

- 🔗 Lack of invoice
- 🔗 Fake invoices
- 🔗 Lack of detail on invoices
- 🔗 Wrong mileage
- 🔗 False mileage
- 🔗 Personal expenses
- 🔗 Alcohol

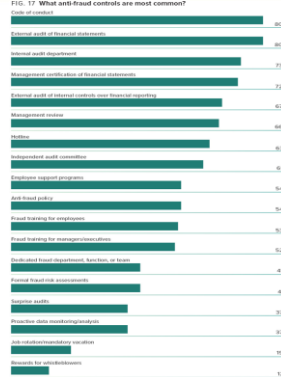
External Frauds

- 🔗 Internet Merchandise Schemes
 - Flash Advertising, spoofing of payment sites
- 🔗 Fake Government Officials
 - IRS
- 🔗 Phishing schemes; more sophisticated
 - Fueled by data breaches (Equifax, Uber)
 - W2 and Wire Scams

Effective Fraud Deterrents

- 🔗 Written Fraud Policy
 - Policy sets expectations
 - Zero Tolerance
 - Review and sign-off by each employee for personnel file
 - Include Reporting Process
 - Whistleblower Protection
 - Issues addressed consistently and timely
- 🔗 Ethics Policy, Conflict of Interest Policy
- 🔗 Training
- 🔗 Continuous Risk Assessment

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



Source: ACFE 2018 Report to the Nations on Occupational Fraud and Abuse

Steps to Reduce Fraud Risk

- ❖ Fraud risk analysis performed
- ❖ Educate
- ❖ Tone at the Top
- ❖ Conflict Disclosures (Council and Management)
- ❖ Establish whistle-blower hotlines
- ❖ Rotation of job duties
- ❖ Zero tolerance
- ❖ Background checks for new hires – don't hire crooks
- ❖ Keep eyes and ears open regarding employee behavior
- ❖ Discuss concerns with auditors
- ❖ Establish effective Internal Audit division
- ❖ Use of Data Mining Software
- ❖ Surprise audits



Highlights

- ❖ Understand the Five Components of Internal Control
- ❖ Everyone is responsible for effective and efficient control development and/or application
- ❖ Train your Team(s)
- ❖ Ongoing evaluation of controls and fraud risk assessment
- ❖ Fraud Statistics
- ❖ Fraud Prevention tips
- ❖ Trust is never a control!



OAPT Conference Understanding Internal Controls & Fraud Prevention June 12, 2018

QUESTIONS?

