OAPT Conference

Understanding Internal Control & Fraud Prevention

June 15, 2021

Presented by:
Derek Conrad, CPA, CFE
Principal, Government Services

Rea & associates
a brighter way

3

Agenda

- Internal Controls
- Fraud Triangle
- Current Fraud Statistics
- Emerging Trends
- Fraud Risk Assessment
- Fraud Prevention Tips

4

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

5

Five components of Internal Control

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

6

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.

7

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

8

Internal Control – Risk Assessment con't

- Management should also focus on the i*nherent 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.

9

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 polices 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
- Polices posted on websites for easy access

10

Internal Control – Information & Communication con't

- Potential issues facing c*ommunication* 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

11

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

12

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.

13

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

14

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

15

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

16

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

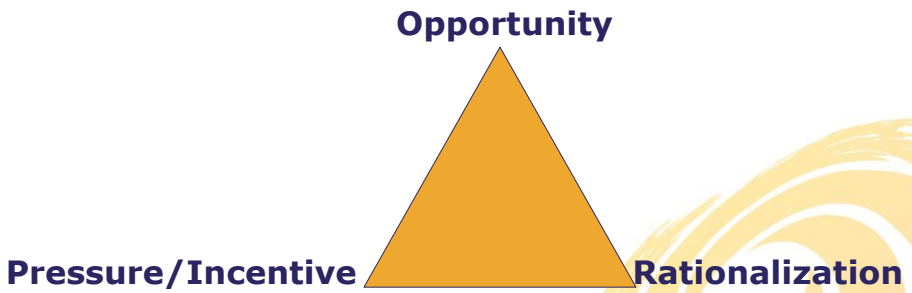
17

Fraud

- Defined by Merriam-Webster
  - → as the intentional perversion of truth in order to induce another to part with something of value or to surrender a legal tight
  - → An act of deceiving or misrepresenting
    - *Intent is the key consideration here.*

18

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

19

Fraud Triangle

- **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")
- **Opportunity –** The ability to commit a fraudulent activity must exist (weaknesses in internal control or the ability to override them)
- **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)

20

Fraud Diamond

David T. Wolfe and Dana R. Hermanson

21

Capability

- 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.

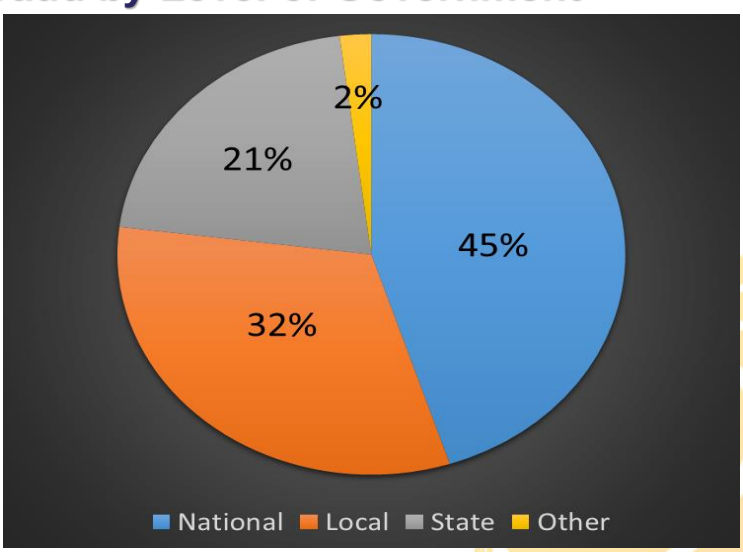
22

Pre-pandemic Fraud Statistics

- Statistics per the ACFE's 2020 Report to the Nations
- Governments continue to be one of the most targeted industries

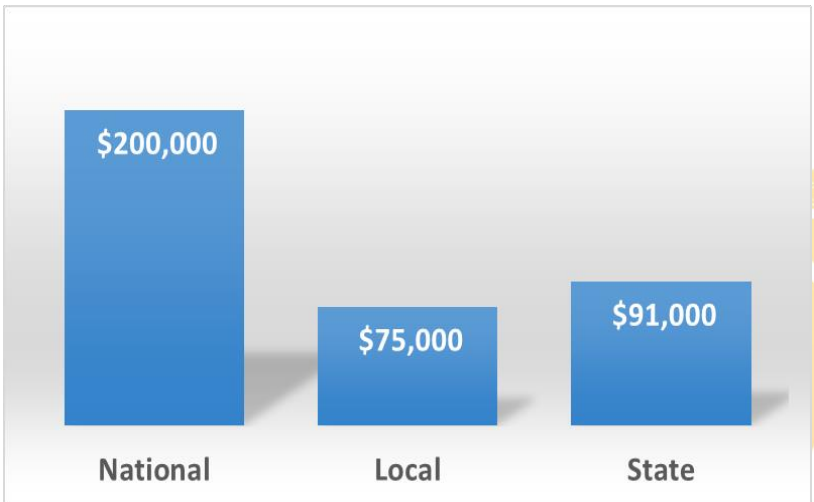
23

Fraud by Level of Government



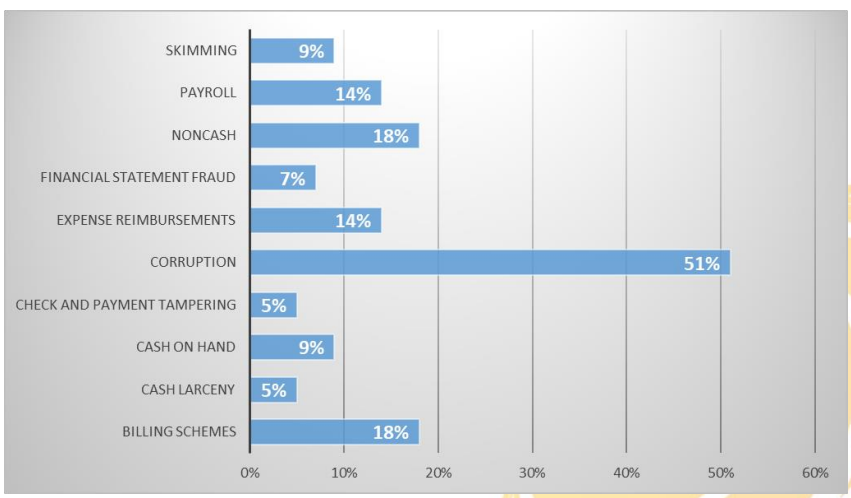
24

Median Loss by Government Type



25

Fraud Cases by Scheme



26

Fraud Schemes

- **Skimming (9%)** – Theft of cash prior to entering into system. "Off the books" fraud.
  - Obviously most common in areas where cash is accepted and limited ability to track activity or number of customers
    - Recreation dept's – pools, concession stands, etc…
- **Payroll (14%)** – Manipulate payroll system to receive payments they haven't earned
  - Timecard fraud
  - Pay rate fraud
  - Ghost employees
  - Withholding theft
  - One of the current, more common themes is fraudsters contacting payroll departments to change employees direct deposit information

27

Fraud Schemes

- **Noncash (18%)** – theft of inventory and equipment, misappropriation of assets
- **Financial Statement (7%)** – Intentional misrepresentation for personal or organizational gain
  - More prevalent where employees receive bonuses for financial performances
  - Increased risk when entities are benchmarked against one another
  - Typically low risk area for governments because little to no incentive to misstate
- **Expense Reimbursements (14%)** – Personal expenses, over-stated expenses, fictitious expenses, double dipping

28

Fraud Schemes

- **Corruption (51%)** – Conflict of interests, kickbacks, contract steering, bid rigging
  - → Typically a much higher dollar amount involved with this type of fraud
  - → More difficult to address internally because typically involves senior management
- **Check and Payment Tampering (5%)** – intercepting, forging or altering checks
- **Cash on Hand (9%)** – theft of petty cash or any other cash on hand.

29

Fraud Schemes

- **Cash Larceny (5%)** – Theft of cash already accounted for in system, "on the books" fraud.
  - → Theft from cash register
  - → Often will involve "adjusting" entries or voided transactions to conceal theft
  - → One of the easier schemes to detect because of the trail left
- **Billing Schemes (18%)** – cause organization to issue fraudulent payments
  - → Shell companies or fictitious vendors
  - → Non-accomplice vendors – existing legitimate vendors but submit fake invoices for payment
  - → Personal purchases on company card.

30

COVID-19 Impact

- Pandemic presented many challenges and increased fraud risks were just one of those challenges
  - → Remote working environment
  - → CARES Act funding created new opportunities
  - → Increased financial pressure and uncertainty
  - → New factors leading to rationalization
  - → Cyber threats increased significantly

31

Emerging fraud risks

- Authorized push (wire transfer) fraud
  - → Often involves social engineering to “tricking” victims to make payments.
  - → Typically a high sense of urgency that leads to improper payments
- Account takeover fraud
  - → Fraudster gains access to account and makes unauthorized transactions.
- Unemployment fraud
  - → Exploded due to CARES Act

32

Emerging fraud risks

- Ransomware continues to be a significant risk
  - → Colonial pipeline
- Less focus on customary transactional fraud and increased focus on data and information
- Cyber environment continues to be biggest risk facing governments
  - → Consider the type of information you currently have, what it could be used for and how it's protected

33

Top 5 Fraud Schemes Predicted to Increase as direct result of pandemic

- 1. Cyberfraud
- 2. Payment Fraud
- 3. Unemployment Fraud
- 4. Fraud by vendors/sellers
- 5. Health Care Fraud

34

Areas where less fraud may be expected

- Cash on hand/skimming – less in-person interaction
- Expense reimbursements – significantly less travel

35

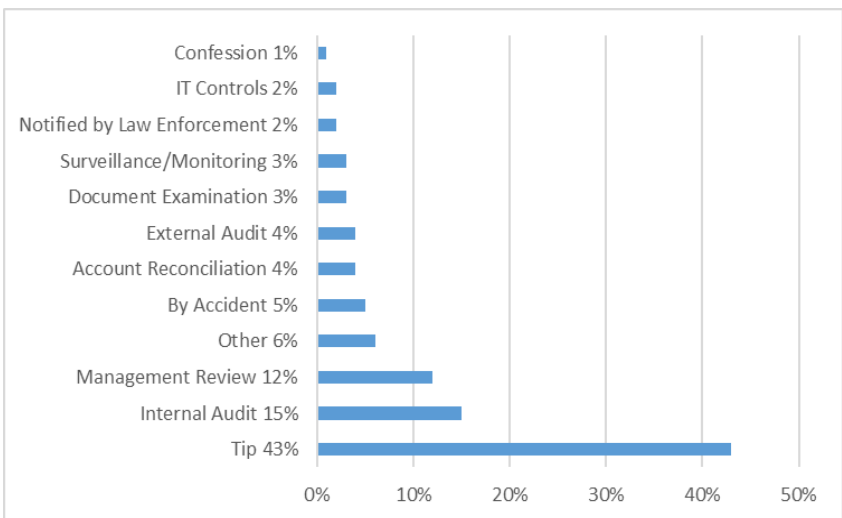
Recent Case Study 1

36

Recent Case Study 2

37

Who's detecting fraud



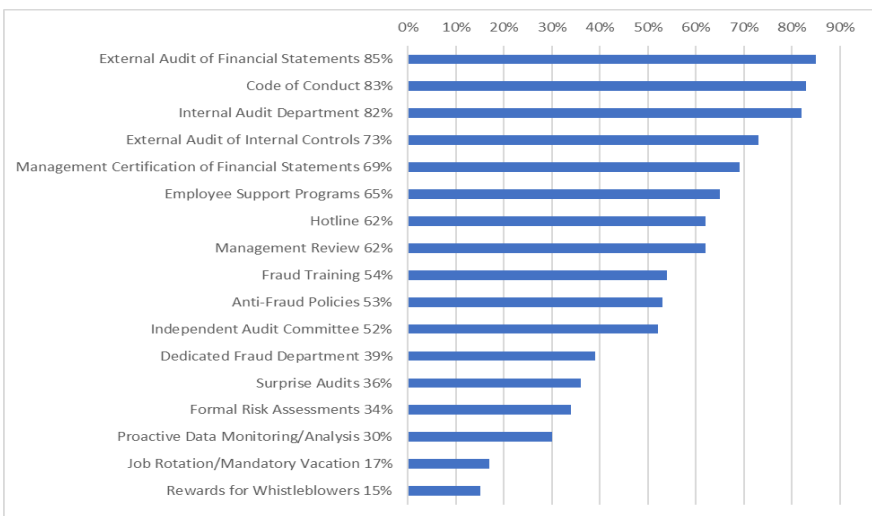
38

Where are the tips coming from?

- Employee – 50%
- Customer – 22%
- Anonymous – 15%
- Vendor – 11%
- Other – 6%
- Competitor – 2%
- Shareholder/Executive – 2%

39

Most commonly cited anti-fraud internal controls



40

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

41

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

42

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

43

Risk Assessment Includes:

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

44

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

45

Risk Identification cont.

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

46

Risk Likelihood

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

47

Risk Response

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

48

Additional considerations for risk assessment

- Who's committing fraud and at what levels of the organization?
- Behavioral Red Flags

49

Fraud by Level of Authority

- 41% of cases identified were committed by an employee – median loss in those cases was $50,000.
- 38% of cases committed by manager – median loss of $135,000.
- 18% of cases committed by an executive – median loss of $264,000.

50

Most common departments for Fraud

- 16% in general operations
- 11% accounting
- 10% executive/upper management
- 8% administrative support
- 7% purchasing

51

Profile of Fraud Perpetrator

- Average age of 45 – age does not appear to be a significant factor
- 73% of frauds noted were committed by men with an average median loss of $142,000.
- Median loss for females was $45,000.

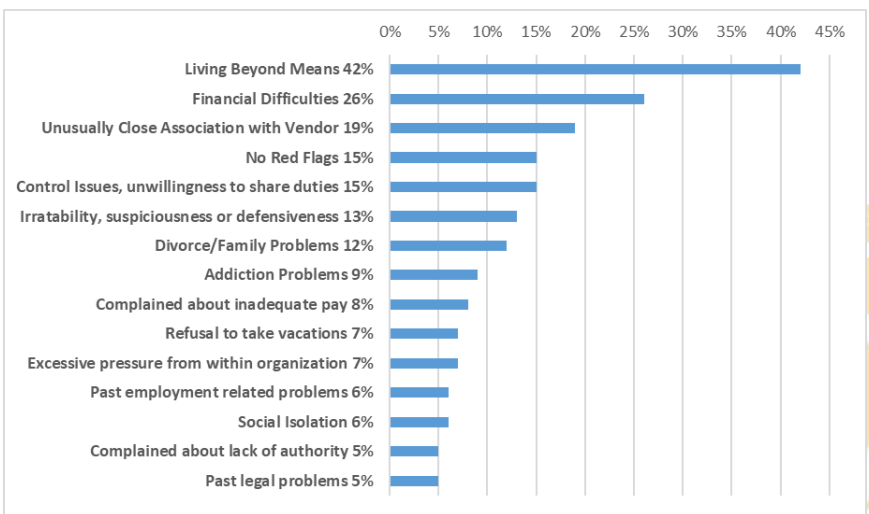
52

Collusion

- 46% of cases involved just one perpetrator with median loss of $69,000
- 54% involved 2 or more people and median losses jump to $250,000

53

Behavioral Red Flags



54

Group Discussion Case 1

55

Group Discussion Case 2

56

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

57

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

58

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

59

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!

60

OAPT Conference

Understanding Internal Controls & Fraud Prevention

June 15, 2021

QUESTIONS?

61