Fraud Risk Management

Introduction

Jeffrey G. Matthews, CFE, CPA
Partner
StoneTurn
CPE Information
Discussion Questions

1. On a scale of 1 to 10 (1 being lowest and 10 being highest), how much emphasis does your organization place on preventing fraud? Detecting fraud? Investigating known instances of fraud?
Discussion Questions

2. Think of an instance of fraud that occurred at your organization (or another organization, if necessary). What were the indirect costs and effects of the fraud?
Discussion Questions

3. Which departments or business activities in your organization present the highest risk of employee theft?

4. What business activities at your organization are most prone to fraudulent misstatements?
Learning Objectives

- Define *fraud* and its components.
- Identify different types of fraud.
- Examine the impact of fraud on organizations.
- Understand why people commit fraud.
- Examine the relationship between anti-fraud initiatives and risk management.
## Foundational Guidance for Managing Fraud Risks

<table>
<thead>
<tr>
<th>Source</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud Risk Management Guide</td>
<td>(COSO and ACFE, 2016)</td>
</tr>
<tr>
<td>Managing the Business Risk of Fraud: A Practical Guide (IIA, AICPA, and ACFE, 2008)</td>
<td></td>
</tr>
<tr>
<td>Internal Control—Integrated Framework</td>
<td>(COSO, 2013)</td>
</tr>
</tbody>
</table>
What Is * Fraud*?

- A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment
Elements of Fraud

- A material false statement
- Knowledge that the statement was false when it was uttered
- Reliance on the false statement by the victim
- Damages resulting from the victim’s reliance on the false statement
Components of Fraud

- The act
- The concealment
- The conversion
Types of Fraud

- Internal/occupational fraud:
  - Asset misappropriation (embezzlement)
  - Corruption
  - Financial statement fraud

- External fraud:
  - Dishonest vendors
  - Dishonest customers
  - Unknown third parties
The Impact of Fraud

- All organizations are susceptible to fraud.
- Fraud is a human problem, not an accounting problem.
ACFE 2018 *Report to the Nations*

- CFEs estimate the typical organization loses 5% of its annual revenue to fraud.
  - Potential total fraud loss of nearly $4 trillion worldwide
- Median loss caused by occupational fraud is $130,000.
- 22% of the frauds involved losses of at least $1 million.
ACFE 2018 Report to the Nations

- **Asset misappropriation schemes:**
  - Most common—89% of cases
  - Least costly—median loss of $114,000

- **Financial statement frauds:**
  - Least common—10% of cases
  - Costliest—median misstatement of $800,000

- **Corruption schemes:**
  - 38% of cases
  - Median loss of $250,000
The Indirect Fallout

- Impact extending well beyond the actual dollar amount stolen
- Loss of employee confidence
- Loss of productivity
- Decline in company image and reputation
Why Do People Commit Fraud?

Fraud Triangle

Opportunity
Pressure
Rationalization
Why Do People Commit Fraud?
When Does the Fraud Triangle Not Apply?

- Predatory employees—those with a premeditated intent of stealing from the employer
- Need for rationalization often dissipates after the first offense
When Does the Fraud Triangle Not Apply?
Why Sanctions Alone Don’t Deter Fraud

- Perpetrators do not anticipate getting caught.
- Perpetrators rationalize their conduct so that it seems legal or justified and thus should not be sanctioned.
- The greatest threat perpetrators face is the detection of their crime.
How Does Fraud Relate to Risk Management?

- *Risk* is the effect (positive or negative) of uncertainty on an organization’s objectives.
How Does Fraud Relate to Risk Management?

- Risks are commonly grouped into the following categories to facilitate risk mitigation:
  - Strategic
  - Operational
  - Reporting
  - Compliance

- Fraud might be a compliance, financial, or operational risk.
How Does Fraud Relate to Risk Management?

- What is risk management?
  - COSO: “the culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value”
  - ISO 31000: “coordinated activities to direct and control an organization with regard to risk”
How Does Fraud Relate to Risk Management?

- Many risk management professionals underestimate the role of fraud in—or even exclude fraud risks from—the scope of their professional duties.
How Does Fraud Relate to Risk Management?

- This course explains how to integrate anti-fraud and risk management initiatives to:
  - Identify, assess, and manage fraud risks.
  - Support fraud risk management by establishing an anti-fraud culture and promoting fraud awareness.
  - Develop a system of internal controls to address fraud risks.
  - Address and respond to identified fraud.
Fraud Risk Management and Internal Control

- Internal Control
- Fraud Risk Management
- Enterprise Risk Management
COSO Definition of *Internal Control*

- *Internal control* is a process, effected by an entity’s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.
Objectives of Internal Control

▪ Operations objectives: the effectiveness and efficiency of the organization’s operations
▪ Reporting objectives: the reporting of financial and nonfinancial information to internal and external parties
▪ Compliance objectives: the organization’s adherence to the laws and the regulations to which it is subject
COSO Internal Control—Integrated Framework

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring
Control Environment

- Sets the moral tone and provides foundation for all other control components

- Principles:
  1. Commitment to integrity and ethical values
  2. Independent board that oversees development and performance of internal control
  3. Appropriate structures, reporting lines, and authorities and responsibilities
  4. Commitment to attract, develop, and retain competent individuals
  5. Accountability for internal control responsibilities
Risk Assessment

- Dynamic and iterative process that forms the basis for determining how risks will be managed

- Principles:
  6. Set sufficiently clear objectives to enable the identification and assessment of risks.
  7. Identify and analyze risks to the achievement of objectives across the entity.
  8. Consider potential for fraud in assessing risks to the achievement of objectives.
  9. Identify and assess changes that could significantly impact the system of internal control.
Control Activities

- Policies and procedures that enforce management’s directives

- Principles:
  10. Select and develop control activities that mitigate risks to acceptable levels.
  11. Select and develop general control activities over technology.
  12. Deploy control activities through policies that establish what is expected and procedures that put policies into action.
The exchange of information in a way that allows employees to carry out their responsibilities and achieve objectives

**Principles:**

13. Obtain or generate and use relevant, quality information to support the functioning of controls.

14. Internally communicate information, including objectives and responsibilities, necessary to support the functioning of internal control.

15. Communicate with external parties regarding matters affecting the functioning of internal control.
Monitoring

- The process that assesses the effectiveness of the control system over time

Principles:

16. Select, develop, and perform ongoing or separate evaluations to ascertain whether the components of internal control are present and functioning.

17. Evaluate and communicate control deficiencies in a timely manner to those parties responsible for taking corrective action.
Business Case for Managing Fraud Risk

- Organizations that deny the true possibility of fraud are at the greatest risk.
Business Case for Managing Fraud Risk

- CFEs estimate that the typical organization loses 5% of its annual revenues to fraud.
- Recovery is typically very little, if any.
- Additional time and money invested in:
  - Investigating how frauds happened
  - Pursuing action against perpetrators
  - Remediating system weaknesses
# Business Case for Managing Fraud Risk

## Median Loss Based on Presence of Anti-Fraud Controls

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

(Source: ACFE 2018 Report to the Nations)
# Business Case for Managing Fraud Risk

## Median Duration of Fraud Based on Presence of Anti-Fraud Controls

<table>
<thead>
<tr>
<th>Control</th>
<th>Percent of cases</th>
<th>Control in place</th>
<th>Control not in place</th>
<th>Percent reduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive data monitoring/analysis</td>
<td>37%</td>
<td>10 months</td>
<td>24 months</td>
<td>58%</td>
</tr>
<tr>
<td>Surprise audits</td>
<td>37%</td>
<td>11 months</td>
<td>24 months</td>
<td>54%</td>
</tr>
<tr>
<td>Internal audit department</td>
<td>73%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Management certification of financial statements</td>
<td>72%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>External audit of internal controls over financial reporting</td>
<td>67%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Management review</td>
<td>66%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Hotline</td>
<td>63%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Anti-fraud policy</td>
<td>54%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Fraud training for employees</td>
<td>53%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Fraud training for managers/executives</td>
<td>52%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Formal fraud risk assessments</td>
<td>41%</td>
<td>12 months</td>
<td>24 months</td>
<td>50%</td>
</tr>
<tr>
<td>Rewards for whistleblowers</td>
<td>12%</td>
<td>9 months</td>
<td>18 months</td>
<td>50%</td>
</tr>
<tr>
<td>Independent audit committee</td>
<td>61%</td>
<td>12 months</td>
<td>23 months</td>
<td>48%</td>
</tr>
<tr>
<td>Code of conduct</td>
<td>80%</td>
<td>13 months</td>
<td>24 months</td>
<td>46%</td>
</tr>
<tr>
<td>Job rotation/mandatory vacation</td>
<td>19%</td>
<td>10 months</td>
<td>18 months</td>
<td>44%</td>
</tr>
<tr>
<td>Dedicated fraud department, function, or team</td>
<td>41%</td>
<td>12 months</td>
<td>20 months</td>
<td>40%</td>
</tr>
<tr>
<td>External audit of financial statements</td>
<td>80%</td>
<td>15 months</td>
<td>24 months</td>
<td>38%</td>
</tr>
<tr>
<td>Employee support programs</td>
<td>54%</td>
<td>12 months</td>
<td>18 months</td>
<td>33%</td>
</tr>
</tbody>
</table>

(Source: ACFE 2018 Report to the Nations)
Business Case for Managing Fraud Risk

- A proactive fraud risk management program:
  - Sends a clear anti-fraud message
  - Demonstrates a sound business strategy
  - Enhances the organization’s image and reputation
  - Promotes goodwill
  - Ensures compliance with laws and regulations
  - Directly increases the bottom line
U.S. Sentencing Guidelines for Organizations

1. Have policies defining standards and procedures that the organization’s agents and employees must follow.

2. Assign specific high-level personnel who have ultimate responsibility to ensure compliance.

3. Use due care not to delegate significant discretionary authority to people whom the organization knew or should have known to have a propensity to engage in illegal activities.
4. Communicate standards and procedures to all agents and employees and require participation in training programs.

5. Take reasonable steps to achieve compliance; for example, by use of monitoring and auditing systems and by having and publicizing a reporting system where employees can report criminal conduct without fear of retribution (hotline or ombudsman program).
U.S. Sentencing Guidelines for Organizations

6. Consistently enforce standards through appropriate discipline, ranging from dismissal to reprimand.

7. After detection of an offense, the organization must have taken all reasonable steps to respond to this offense and prevent further similar offenses—including modifying its program and appropriately disciplining individuals responsible for the offense and those who failed to detect it.
U.S. Sentencing Guidelines for Organizations

- The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement set forth in [the seven elements] to reduce the risk of criminal conduct identified through this process.