Fraud Risk Assessment
A Key Element of an Effective Anti-Fraud Program
Meet Our Presenters

Deron Rossi, CFS
Fraud Consultant
Risk & Compliance Services

Tim Lietz, CIA, CRMA
National Practice Director
Risk & Compliance Services
Agenda

1. Current Fraud Landscape/Background Information
2. Anti-Fraud Program and Controls
3. Fraud Risk Assessment – Approach and Methodology
4. Fraud Risk Assessment Best Practices and Tools
Polling Question #1

Which functional area do you represent at your firm?

A. Internal Audit
B. Risk Management
C. Executive Management
D. Finance/Other
HERE’S THE ETHICS STUFF. IT’S ALL THERE – JUST SIGN ON THE LAST PAGE.
Current Fraud Landscape
IIA Three Lines Model

GOVERNING BODY
Accountability to stakeholders for organizational oversight

Governing body roles: integrity, leadership, and transparency

MANAGEMENT
Actions (including managing risk) to achieve organizational objectives

First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters

INTERNAL AUDIT
Independent assurance

Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives

KEY:
↑ Accountability, reporting
↓ Delegation, direction, resources, oversight
↔ Alignment, communication coordination, collaboration
Three core concepts when taken together, create a situation ripe for fraud.

1. **Pressure** – Think motive - financial, personal vices or other pressures

2. **Rationalization** – Important component of most frauds; people need to reconcile their behavior (ex. I am underpaid, I deserve this.)

3. **Opportunity** – Open door for solving a non-shareable problem in secret by violating a trust relationship; accomplished by generally weak or no controls

Each element must co-exist with the other.
2020 Fraud Statistics

CFEs estimate that organizations lose 5% of revenue to fraud each year.

**Median Loss per Case:** $125,000

**Average Loss per Case:** $1,509,000

**Asset Misappropriation Schemes** are the most common and least costly.

- 86% of cases
- Median loss: $100,000

**Financial Statement Fraud Schemes** are the least common and most costly.

- 10% of cases
- Median loss: $954,000

*2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.*
2020 Fraud Statistics

Fig. 6 How does the duration of a fraud relate to median loss?

<table>
<thead>
<tr>
<th>PERCENT OF CASES</th>
<th>MEDIAN LOSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>≤6 months</td>
<td>$50,000</td>
</tr>
<tr>
<td>7-12 months</td>
<td>$90,000</td>
</tr>
<tr>
<td>13-18 months</td>
<td>$135,000</td>
</tr>
<tr>
<td>19-24 months</td>
<td>$210,000</td>
</tr>
<tr>
<td>25-36 months</td>
<td>$300,000</td>
</tr>
<tr>
<td>37-48 months</td>
<td>$430,000</td>
</tr>
<tr>
<td>49-60 months</td>
<td>$340,000</td>
</tr>
<tr>
<td>&gt;60 months</td>
<td>$740,000</td>
</tr>
</tbody>
</table>

2020 Report to the Nations. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.
2020 Fraud Statistics

USE OF TARGETED ANTI-FRAUD CONTROLS HAS INCREASED OVER LAST DECADE

- HOTLINE: 13%
- ANTI-FRAUD POLICY: 13%
- FRAUD TRAINING FOR EMPLOYEES: 11%
- FRAUD TRAINING FOR MANAGERS/EXECUTIVES: 9%

A lack of internal controls contributed to nearly 1/3 of frauds.

THE PRESENCE OF ANTI-FRAUD CONTROLS IS ASSOCIATED WITH LOWER FRAUD LOSSES AND QUICKER DETECTION.
Polling Question #2

What percentage of revenue is believed to be lost to an organization due to occupational fraud?

A. 15%
B. 8%
C. 5%
D. 2%
Increases of Fraud During the Pandemic

- Economic Pressure
- Unfilled Positions
- Increased Stress and Uncertainty
- Record Phishing/Smishing
- Job Roles Changing for People Still Employed
- System Access Overlaps with New Roles
- Segregation of Duties Challenges
- Working in Isolation
- Distracted Management
Control / Risk Focal Points for 2022

1. The Three Lines work collaboratively to holistically look at risk, including identifying new risk that emerged over past 24 months. Continue to adjust 2022 Plan as needed

2. Reiterate Tone at the Top Messaging Addressing Ethical Challenges

3. Economic conditions, including inflationary pressures, constrained growth opportunities

4. What critical projects affecting controls and risk were put on hold and might not be addressed?

5. Usage of RPA, AI or other process enhancements?

6. Third Party risks

7. Cyber, cyber, cyber

8. Employee flight risks
Polling Question #3

*What are the biggest risks that you are focused on in 2022?*

A. Fraud Risk
B. Cybersecurity Risk
C. Third Party Management Risk
D. Environment, Social, Governance (ESG) Risk
E. Talent Acquisition and Retention
Anti-Fraud Program and Controls
Anti-Fraud Programs and Controls

**Preventive**
- Tone at the Top
- Effective Governance
- Code of Ethics / Conduct
- Culture of Ethics and Integrity
- Positive Working Environment
- **Fraud Risk Assessment**
- Fraud Policy
- Internal Controls
- Employee and Third-Party Due Diligence
- Training (New Hire & On-going)

**Detective**
- Whistleblower Program (Hotline)
- Internal Controls
- Internal Audit Function
- Compliance / Risk Management Functions
- Continuous Monitoring by Management

**Responsive**
- Investigation and Remediation
- Enforcement Practices
- Demonstrated Accountability
- Disclosure Practices
**Fraud Risk Assessment Background and Objectives**

<table>
<thead>
<tr>
<th>COSO 2013 INTERNAL CONTROL FRAMEWORK</th>
<th>OBJECTIVES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommends every organization consider the potential for fraud in assessing risk as part of internal control.</td>
<td>Inform Senior Management and the Audit Committee about the existence of any significant fraud risks.</td>
</tr>
<tr>
<td>It is anticipated that such an assessment will be refreshed annually and discussed with the Audit Committee.</td>
<td>Assess how fraud risks are being mitigated.</td>
</tr>
</tbody>
</table>
| COSO Principle 8 - “Assess Fraud” - Lists the four primary fraud risk considerations  
  1. Fraudulent reporting  
  2. Safeguarding of assets  
  3. Corruption  
  4. Management Overrides | Determine if any significant fraud risks are NOT being addressed by a company’s existing controls and specific fraud prevention programs. |
Polling Question #4

*How often does your firm perform a fraud risk assessment?*

A. Annually  
B. Every Other Year  
C. Every 3-5 Years  
D. Within the Last Decade  
E. Never
Fraud Risk Assessment Participants

**Accounting/Finance**
Familiar with the financial reporting process and internal controls

**Non-Financial Business Unit and Operations**
Leverage their knowledge of day-to-day operations, customer and vendor interactions, and general awareness of issues within the industry

**Legal & Compliance**
The fraud risk assessment will identify risks that give rise to potential criminal, civil, and regulatory liability if the fraud or misconduct were to occur

**Risk Management**
Ensure the fraud risk assessment process integrates with the organization’s ERM program

**Internal Audit**
Familiar with the organization’s internal controls and monitoring functions; integral in developing and executing responses to significant risks that cannot be mitigated practically by preventive and detective controls
5-Step Fraud Risk Assessment Methodology

1. Define the risk assessment universe and fraud categories

2. Identify potential fraud schemes in each area

3. Rate/Score the “Likelihood” and “Significance” of each identified fraud scheme

4. Link fraud risks rated as “High” to existing controls and identify risks not being mitigated by existing controls

5. Develop remediation plans to address identified gaps and implement appropriate responses
Fraud Risk Assessment Tool Examples

Scoring “Likelihood” and “Significance”

Likelihood
Management’s assessment of the likelihood of a fraud risk occurring is informed by instances of that particular fraud occurring in the past at the organization, the prevalence of the fraud risk in the organization’s industry, the organization’s overall control environment, and other factors, including the number of individual transactions, the complexity of the risk, and the number of people involved in reviewing or approving the process.

Rating Scale

<table>
<thead>
<tr>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote</td>
<td></td>
<td>Reasonably Possible</td>
<td></td>
<td>Probable</td>
</tr>
</tbody>
</table>

Significance
The assessment of the significance of a fraud risk should include not only financial statement and monetary significance, but also significance to an organization’s operations, brand value, and reputation, as well as criminal, civil, and regulatory liability. For example, two different organizations may have similar amounts of expenses charged via employee expense reports, but one organization is a professional services firm that charges those expenses to clients. Although the likelihood of the risk of fraudulent expense reports and the monetary exposure may be similar at both organizations, the relative significance of fraudulent expense reports to the professional services firm may be greater, given the impact that fraudulent expense reports can have on customer relationships.

Rating Scale

<table>
<thead>
<tr>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inconsequential</td>
<td></td>
<td>Significant</td>
<td></td>
<td>Material</td>
</tr>
</tbody>
</table>
Lessons Learned / Best Practices / Tools
The foundations of an effective fraud risk management program are rooted in a risk assessment, overseen by the board, which identifies where fraud may occur within the organization.

A fraud risk assessment should be performed on a systematic and recurring basis, involve appropriate personnel, consider relevant fraud schemes and scenarios, and mapping those fraud schemes and scenarios to mitigating controls.

Also done in response to allegations or suspicions.

The existence of a fraud risk assessment and the fact that management is articulating its existence may even deter would-be fraud perpetrators.

An effective Fraud Risk Assessment will identify previously unidentified risks and strengthen the ability of the organization to prevent and detect fraud and misconduct.

Increased importance with SAS 99, AS5 and SEC guidance for management on SOX 404.

Controls designed to mitigate high fraud risks are “key”.

Absence of a Fraud Risk Assessment could result in a “Significant Deficiency”.

Critical component of effective Anti-Fraud Programs and Controls.
To protect itself and its stakeholders effectively and efficiently from fraud, an organization should understand fraud risk and the specific risks that directly or indirectly apply to the organization.

A structured fraud risk assessment, tailored to the organization’s size, complexity, industry, and goals, should be performed and updated periodically.

The assessment may be integrated with an overall organizational risk assessment or performed as a stand-alone exercise, but should, at a minimum, include risk identification, risk likelihood and significance assessment, and risk response.

An effective fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud.

Employee incentive programs and the metrics on which they are based can provide a map to where fraud is most likely to occur.

Fraud risk assessment should consider the potential override of controls by management as well as areas where controls are weak or there is a lack of segregation of duties.

An initial assessment of fraud risk should consider the inherent risks of a particular fraud in the absence of any assumed controls that may address the risk.
Fraud Risk Management – Guidance / Best Practices
Fraud Risk Assessment Best Reference Tools

• ACFE / AICPA Fraud Risk Management Toolbox
• ACFE 2020 Report to the Nations (next release scheduled for 2022)
• ACFE / IIA / AICAP Fraud Risk Management Guidance
• ACFE / Grant Thornton Anti-Fraud Playbook
• IIA / GTAG 13: Fraud Prevention and Detection in an Automated World
• IIA Practice Guide – Internal Auditing and Fraud
• COSO / ACFE Fraud Risk Management Guide
Q&A / Contact Info

Deron Rossi
Fraud Consultant
Risk & Compliance Services
919.417.3061
deron.rossi@jeffersonwells.com

Tim Lietz
National Practice Director
Risk & Compliance Services
336.706.2030
timothy.lietz@jeffersonwells.com

THANK YOU FOR ATTENDING!