Speakers

James Ruotolo
Senior Manager
Fraud Risk Mitigation & Analytics
Grant Thornton
James.Ruotolo@us.gt.com
@jdruohtolo

Holly Johnson
Senior Manager
Forensic Advisory Services
Grant Thornton
Holly.Johnson@us.gt.com
Learning objectives

1. Describe the five key principles of COSO Fraud Risk Management Guide
2. Identify the ten playbook "plays" to implement the COSO FRM principles
3. Locate and apply supplemental fraud risk management tools
What We Will Cover

1. Introduction
2. The Phases & Plays
3. Q&A
How Did We Get Here?

1992
COSO releases its original Internal Control-Integrated Framework

2013
COSO incorporates 17 principles, including a new principle focused on fraud risk

2016
COSO & ACFE publish the Fraud Risk Management Guide

2020
Grant Thornton & ACFE publish the Anti-Fraud Playbook
COSO’s Fraud Risk Management Principles

Fraud Risk Governance: The organization establishes and communicates a Fraud Risk Management program

Fraud Risk Assessment: The organization performs comprehensive fraud risk assessment

Fraud Control Activity: The organization selects, develops, and deploys preventive and detective fraud control activities

Fraud Investigation & Corrective Action: The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action

Fraud Risk Management Monitoring Activities: The organization selects, develops, and performs ongoing evaluations
The Anti-Fraud Playbook

The playbook is intended to provide practical guidance for organizations looking to begin, advance, or benchmark their Fraud Risk Management (FRM) programs against best practices.

It draws on insights from the COSO Guide and seeks to clarify and operationalize the concepts put forward in that guidance. The playbook includes key questions, checklists, and insights that will enhance your FRM program and ultimately facilitate effective and proactive FRM at your organization.
The Phases & Plays
The Phases & Plays

**Fraud Risk Governance**
- Play #1 – Understand Where You Are & Where You Want to Be
- Play #2 – Create a Culture

**Fraud Monitoring**
- Play #9 – Monitor Your Progress
- Play #10 – Report on Your Progress

**Investigations and Corrective Action**
- Play #7 – Lay the Groundwork for Investigations
- Play #8 – Conduct Investigations

**Fraud Risk Assessment**
- Play #3 – Think Like a Fraudster
- Play #4 – Discover What You Don’t Know

**Fraud Control Activities**
- Play #5 – Use Data to Uncover Fraud
- Play #6 – Knowledge is Power
Fraud Risk Management (FRM) should be right-sized and tailored for the unique needs of each organization.

An organization must understand where their FRM program stands today (current state), then identify their long term vision (goal state).

This process will allow you to develop a roadmap for the future and focus on gaps that need to be addressed to move from the current to the goal state, ensuring resources are effectively utilized in areas of high impact and high priority.
Fraud Risk Governance
Play 2: Create a Culture

Promoting fraud awareness throughout your organization from the top down is vital to creating a strong anti-fraud culture, enhancing fraud awareness, and encouraging employees to discuss fraud risks openly and thoughtfully.

There is not a one-size-fits-all model when it comes to promoting fraud awareness. It is important for every organization to tailor these efforts to be relevant to its specific fraud risks and the strategic goals of the FRM program.

Serving as the counterbalance to the Fraud Triangle, the Integrity Triangle emphasizes the values that encourage people to do what is right for the organization.
The ACFE conducts an extensive bi-annual survey known as the “Report to The Nations” regarding occupational fraud. The 2020 report detailed the following findings:

- > $3.6 Billion total losses reported covering 2,504 cases across the world from 125 countries.
- $8,300 per month lost in typical fraud cases which may last 14 months before detection.
- $1.5 Million average losses reported per case.
- 86% of cases are related to asset misappropriation schemes and have a median loss of $100,000.
- 5% of organization’s revenue lost to fraud each year, estimated by CFEs.
- 10% of cases are related to financial statement fraud schemes with a median loss of $954,000.
Fraud Risk Governance
Play 2: Create a Culture – Employee Responsibility

- Association of Certified Fraud Examiners estimates that **43% of internal frauds are identified by tips from co-workers**
- Data is available for analysis to seek out non-conforming behavior
- **Customers and vendors complain** to front line operation folks (this is often a warning sign)
- Every employee function should have a back-up (there is a good reason to require that personnel take vacations)
- Work side by side with employees who might be tempted
- Respect an organization's policies and procedures
- **Continue seeking training** and further education about organizational risks
- Avoid shortcuts for convenience or a favor for a colleague
- Report upwards when pressured by supervisor/management

Grant Thornton
Fraud Risk Governance

Play 2: Create a Culture – Don’t Blame The Auditors

There is often an expectation that auditors have responsibility for fraud prevention and detection.

While auditors doubtless have a role to play in fraud risk management, they do not have primary responsibility. This lies with management and those charged with governance of the organization. It requires auditors to:

- discuss the risk of fraud with management and those charged with governance
- discuss with the audit team the susceptibility of the accounts to material misstatements due to fraud
- perform audit procedures to address the risk of management override
- test journal entries and review accounting estimates for bias
- understand the business rationale for transactions outside the normal course of business
- test the organization’s fraud risk management program and related fraud-related key internal controls on a least an annual basis
- test results of ethics hotline and key internal controls on a quarterly basis as results are provided to the Board of Directors
Fraud Risk Governance
Play 2: Create a Culture – The Control Environment

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.

**Control Environment**

- The organization demonstrates a commitment to integrity and ethical values.
- The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
- Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
- The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
Prevention starts with effective internal controls – however a sound system of internal control can not provide complete protection against all fraudulent behavior, highlighting the importance of fraud prevention and fraud detection measures. Prevention also includes adopting methods that decrease motive, restrict opportunity, and limit the ability for potential perpetrators to rationalize their actions. Examples of key fraud prevention measures include:

- Policies
- Procedures
- Internal controls
- Training
- Fraud awareness communications

**Internal controls** to minimize fraud should, where possible, address fraud "red flags". Examples of the variety of such controls include:

- requiring multiple signatories on high value transactions
- enforcing employees to take vacation (e.g., two weeks core leave)
- restricting belongings that can be brought into the office environment (e.g., many call center employees are not allowed to take in pens, paper, or mobile phones, and some organizations have restricted the use of USB sticks)
- conducting random searches
## Fraud Control Environment
### Play 2: Create a Culture – Relevant IIA Standards

The Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing* includes several fraud-related standards within their International Professional Practices Framework (IPPF).

<table>
<thead>
<tr>
<th>IIA Standard</th>
<th>Description</th>
<th>Interpretation / Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1210 - Proficiency</td>
<td>Internal auditors must possess the knowledge, skills, and other competencies needed to perform their individual responsibilities. The internal audit activity collectively must possess or obtain the knowledge, skills, and other competencies needed to perform its responsibilities.</td>
<td>1210.A2 – Internal auditors must have sufficient knowledge to <em>evaluate the risk of fraud</em> and the manner in which it is managed by the organization, but are <em>not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.</em></td>
</tr>
<tr>
<td>1220 - Due Professional Care</td>
<td>Internal auditors must apply the care and skill expected of a reasonably prudent and competent internal auditor. Due professional care does not imply infallibility. 1220.A1 – Internal auditors must exercise due professional care by considering the:   - Extent of work needed to achieve the engagement’s objectives.   - Relative complexity, materiality, or significance of matters to which assurance procedures are applied.   - Adequacy and effectiveness of governance, risk management, and control processes.   - Probability of significant errors, fraud, or noncompliance.   - Cost of assurance in relation to potential benefits.</td>
<td>N/A</td>
</tr>
<tr>
<td>2060 - Reporting to Senior Management and the Board</td>
<td>The chief audit executive must report periodically to senior management and the board on the internal audit activity’s purpose, authority, responsibility, and performance relative to its plan and on its conformance with the Code of Ethics and the Standards. Reporting must also include significant risk and control issues, <strong>including fraud risks</strong>, governance issues, and other matters that require the attention of senior management and/or the board.</td>
<td>The frequency and content of reporting are determined collaboratively by the chief audit executive, senior management, and the board. The frequency and content of reporting depends on the importance of the information to be communicated and the urgency of the related actions to be taken by senior management and/or the board.</td>
</tr>
</tbody>
</table>
### Fraud Control Environment

**Play 2: Create a Culture – Relevant IIA Standards Cont.**

The Institute of Internal Auditors (IIA) *International Standards for the Professional Practice of Internal Auditing* includes several fraud-related standards within their International Professional Practices Framework (IPPF).

<table>
<thead>
<tr>
<th>IIA Standard</th>
<th>Description</th>
<th>Interpretation / Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>2120 – Risk Management</td>
<td>The internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes.</td>
<td>Risk management processes are monitored through ongoing management activities, separate evaluations, or both. 2120.A2 – The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.</td>
</tr>
<tr>
<td>2210 – Engagement Objectives</td>
<td>Objectives must be established for each engagement. 2210.A1 – Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment. 2210.A2 – Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives. 2210.A3 – Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board. 2210.C1 – Consulting engagement objectives must address governance, risk management, and control processes to the extent agreed upon with the client. 2210.C2 – Consulting engagement objectives must be consistent with the organization's values, strategies, and objectives.</td>
<td>Types of criteria may include:  □ Internal (e.g., policies and procedures of the organization). □ External (e.g., laws and regulations imposed by statutory bodies). □ Leading practices (e.g., industry and professional guidance).</td>
</tr>
</tbody>
</table>
Fraud Risk Assessment

Play 3: Think Like a Fraudster

Identifying vulnerabilities and likely fraud schemes – both internal and external – is imperative to informing your fraud risk assessment.

Thinking like a fraudster and brainstorming the various fraud schemes that could be used to commit fraud within or against your organization is a key step.

You can accomplish this effort by developing a comprehensive Fraud Risk Map, which identifies significant fraud scenarios across your entire organization.
### Fraud Risk Assessment

#### Play 3: Think Like a Fraudster

<table>
<thead>
<tr>
<th></th>
<th>Asset Misappropriation</th>
<th>Financial Misstatement</th>
<th>Corruption</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Perpetrator</strong></td>
<td>- Any employee</td>
<td>- Management &amp; financial reporting</td>
<td>- Procurement, supply chain, inventory control, sales</td>
</tr>
<tr>
<td></td>
<td>- Sole actor or collaborators</td>
<td>- Collusion required</td>
<td>- Individual employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- External party</td>
</tr>
<tr>
<td><strong>Scale</strong></td>
<td>Small $ to Millions</td>
<td>Millions to Billions</td>
<td>Small to Midsize $</td>
</tr>
<tr>
<td><strong>Rewards</strong></td>
<td>- Cash enrichment</td>
<td>- Performance bonuses</td>
<td>- Cash enrichment</td>
</tr>
<tr>
<td></td>
<td>- Inventory or Fixed Assets</td>
<td>- Promotions</td>
<td>- Gift or trips</td>
</tr>
<tr>
<td></td>
<td>- Employee resources</td>
<td>- Attract new investors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Build brand perception</td>
<td></td>
</tr>
<tr>
<td><strong>Goals</strong></td>
<td>- Enrich Employee</td>
<td>- Manipulate actual results</td>
<td>- Provide preferential status to certain vendor(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Falsify existence of events</td>
<td>- Allow for monopolistic supplier or price inflation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Suppress existence of actual events</td>
<td>- Enrich employee</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fraud Risk Assessment

Play 4: Discover What You Don’t Know

Conducting a fraud risk assessment helps you understand exactly where your processes may be vulnerable to fraud and allows for a holistic and detailed look at the fraud risks across the organization.

A Fraud Risk Assessment is a tool that helps organizations identify the unknowns through the identification of key risks – both internal and external – and enables organizations to take action to proactively combat those risks.

Grant Thornton
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.

**Risk Assessment**

- The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

- The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

- The organization considers the potential for fraud in assessing risks to the achievement of objectives.

- The organization identifies and assesses changes that could significantly impact the system of internal control.
As you develop a methodology and conduct a fraud risk assessment, key questions to ask yourself include:

- Who will be on your fraud risk assessment team? What are their roles and responsibilities?
- Where do you want to start your fraud risk assessment?
- Does your organization leverage a likelihood and impact scale for other risk assessment efforts that you can leverage for assessing fraud risk? If not, how do you plan to develop those scales?
- How will you educate stakeholders on the fraud risk assessment process to ensure understanding of key terms and procedures?
- How will you document and evaluate existing anti-fraud controls throughout the assessment process?
- What factors should you consider when prioritizing fraud risks? Will this be based solely on likelihood and impact scores, or will other information be considered?
- How will you respond to high-priority risks identified? How can you leverage your roadmap and strategy (see Play 1) to inform this process?
- How often will you perform a fraud risk assessment? What changes will initiate a reassessment?
As part of the risk scoring process, you should identify existing anti-fraud controls and their effectiveness. This will help determine likelihood and impact scores and inform risk response.
Fraud Control Activities

Play 5: Use Data to Uncover Fraud

FRAUD RISK ASSESSMENT

- Rule-based analytics
- Anomaly detection analytics
- Predictive analytics
- Network / link analytics
- Text analytics

- Known patterns
- Unknown patterns
- Complex patterns
- Linked patterns
- Text patterns

Common fraud
Criminal fraud
Organized fraud
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.

Control Activities

- The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

- The organization selects and develops general control activities over technology to support the achievement of objectives.

- The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.
Fraud Control Activities
Play 5: Use Data to Uncover Fraud – Anomaly Detection

An effective fraud detection strategy involves different types of procedures, including analytical, to **highlight anomalies** – and the introduction of reporting mechanisms that provide for communication of suspected fraudulent acts. Key elements of an effective fraud detection system typically include:

- Exception reporting
- Data mining
- Trend analysis
- Ongoing risk assessment

Examples of the type of fraud analysis for ACH and wire monitoring include:

- Average dollar amount
- Transactions under established requirement thresholds (e.g., $10k, $50k, $100k)
- Average frequency / activity spike notification
- New or atypical recipient location
- New accounts with large deposits
- Dormant accounts / newly active
- New / high-risk country reporting
- Recipients as cash-operated businesses
Fraud Control Activities
Play 6: Knowledge is Power

Organizations should not only develop and deploy mandatory enterprise-wide anti-fraud training, but customize the content and delivery of the training.

This type of targeted and role-based anti-fraud training will help your employees to better identify suspicious activity and feel empowered to act against potential fraud.

Focus on real-life examples and provide on-the-job tools, such as red flags listings or job aides. Include interactive sessions, such as role-playing exercises to keep participants engaged and help employees practice the thoughts and behaviors demonstrated in the training materials.

Still not convinced that you need this type of training?

Tips are time and time again one of the top ways that fraud is identified. The ACFE’s 2020 Report to the Nations found that organizations with fraud awareness training for employees were more likely to get tips through formal reporting mechanisms, 56% compared to 37%. That translates to more effective hotlines and the potential to catch fraud sooner, reducing the loss and impact to your organization.
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.

**Information & Communication**

- The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.

- The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

- The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.
## Fraud Control Activities
### Play 6: Knowledge is Power – Red Flags

<table>
<thead>
<tr>
<th>Operational Issues</th>
<th>Cultural Issues</th>
<th>Financial Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Weak internal control environment</td>
<td>• Employees living beyond their means</td>
<td>• Increasing A/R compared to cash</td>
</tr>
<tr>
<td>• Lack of account reconciliations</td>
<td>• Family members of leadership employed by the organization</td>
<td>• Flat or declining sales with increasing cost of sales</td>
</tr>
<tr>
<td>• Customer billing and payment complaints</td>
<td>• Frequent turnover of accounting personnel</td>
<td>• Increasing &quot;soft&quot; expenses (like &quot;temporary labor&quot;, &quot;consulting&quot;, &quot;advertising&quot;)</td>
</tr>
<tr>
<td>• Numerous credit memos issued to clients of one sales representative</td>
<td>• Management compensation depends on meeting quantified targets</td>
<td>• “Eternal” reconciling items</td>
</tr>
<tr>
<td>• Vendor name consists of initials or vague business purpose</td>
<td>• Organization has engaged in opinion shopping</td>
<td>• Organization undergoes frequent structural re-organizations</td>
</tr>
<tr>
<td>• Excessive &quot;void&quot;, missing or destroyed checks</td>
<td>• Large number of related party relationships</td>
<td>• Organization always meets revenue projections</td>
</tr>
<tr>
<td>• Unsecured signature stamp or electronic signatures</td>
<td>• Poor tone at the top</td>
<td>• Organization often reports financial results &quot;at the last minute&quot; or late</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fraud Control Activities
Play 6: Knowledge is Power – Develop a Plan

- **When an occurrence of fraud is first suspected**, a response should be fashioned based on the organization’s written contingency plan.

- Creating a fraud contingency plan should be a **collaborative effort** that incorporates the needs, concerns, and priorities of the following individuals or groups:
  - General Counsel
  - Internal Audit department
  - Risk Management department
  - Chief Financial Officer(s)
  - Senior operational management
  - Chief Executive Officer
  - Audit Committee/Board of Directors

Fraud Contingency Plan Check List
- Inform attorney
- Notify insurance company
- Notify audit committee/BOD
- Identify company objectives
- Identify sources of restitution
- Inform proper authorities
- Interview suspected employee(s)
- Preserve potential evidence
- Isolate continued risks
- Safeguard the premises
- Communicate event Company-wide
- Communicate event outside Company
- Gather information from outside parties
A Fraud Contingency Plan will allow your organization to employ a consistent and comprehensive response to suspected and detected incidents of fraud. This sends a message that fraud is taken seriously and that action will be taken against the perpetuators. Each case that is detected and investigated creates a deterrent and acts as a form of fraud prevention.

Some effective response methods include:

• Preserving evidence for prosecution
• Conducting thorough investigations
• Taking statements from witnesses or suspects
• Reviewing existing systems to investigate system flaws and implementing changes
• Creating and distributing an annual fraud report
• Disciplining the individuals responsible through internal, civil, or criminal action
An effective fraud risk management framework include controls that first **prevent** fraud from occurring, **detect** fraud when it does happen and **respond** effectively to fraud incidents when they occur. **Investigations are part of fraud response.**

A **necessary first step** is to **lay the proper foundations** for such an investigation by adopting the proper tools and mechanisms to **evaluate**, **communicate**, and **remediate** both instances of potential fraud and the control deficiencies that lead to fraud.

This will **empower your organization to prioritize, assign, and monitor reported fraud** and implement effective corrective actions.
Fraud can be perpetrated through a variety of avenues, each with differing indicators that may suggest whether your company is under a high risk environment.

Understanding the signs relating to differing fraud schemes will allow you to take the appropriate actions quickly.
Investigations & Corrective Action
Play 7: Lay the Groundwork for Investigations – The Team

Benefits of The Team
Experience to competently perform
Objective in fact and appearance
Complete and thorough
Privilege
Investigations & Corrective Action

Play 8: Conduct Investigations

Investigations are a critical component of uncovering not only fraud within your organization, but also a range of associated other corporate crimes, such as money laundering, corruption, and bribery. Investigations also act as an effective fraud deterrence practice, showcasing the organization’s commitment to high ethical standards and creating the perception of detection.

If you have a solid foundation, as highlighted in the previous play, then this should be a well-defined process. Key steps you should perform following the conclusion of an investigation include: communicating investigation results, taking corrective action, and finally, evaluating investigation performance.
Investigations & Corrective Action

Play 8: Conduct Investigations – Legal Considerations

The Attorney Client Privilege

- Refers to a legal privilege that works to keep confidential communications between an attorney and his or her client secret.

The Work-Product Doctrine

- States that an adverse party generally may not discover or compel disclosure of written or oral materials prepared by or for an attorney in the course of legal representation, especially in preparation for litigation.

Interviews: Right to Representation

- The interviewer is not required to provide legal representation nor advis the right to representation. Rules vary when union members are involved.

Interviews: Upjohn Warnings

- If a lawyer is conducting the interview, they must provide the Upjohn Warning also known as the Corporate Miranda Warning. The notice informs the employee that the attorney represents only the company and not the employee individually.
In regard to relevant legal considerations, the following best practices should be taken to protect privileges:

- Ask the lawyers involved how they want you to communicate with them and the client
- Prominently mark documents as “Attorney-Client Privileged” or “Work Product”
- Limit documents to only those involved in privileged communications
- Don’t discuss the case outside of those counsel deems necessary
Investigations & Corrective Action
Play 8: Conduct Investigations – Investigation Goals

• Conduct with the right scope & procedures to answer:
  • What happened and during what time period?
  • Who was involved?
  • Why and how it happened?
  • What was the impact?

• Minimize disruption to business operations
• Perform the investigation as efficiently as possible
• Suggest potential remedial actions
• Respond to interested parties (external auditors, SEC etc.)
• Complete the investigation with no restrictions on scope
During the initial assessment, investigators should be aware of the following common mistakes:

- Underestimate the allegation
- Timing and Structure
- Underestimate internal human resource issues
- Internal Resource Capacity
- Effect on Performance and Morale
- Role of External Auditor
# Investigations & Corrective Action

## Play 8: Conduct Investigations – Key Considerations

### Confidentiality
- Damage to someone’s reputation if others hear of allegation
- Success of investigation can be undermined
- Subjects(s) could attempt to cover up
- Liability of negative publicity

### Competence
- Strong interview skills
- Proper documentation
- Awareness of all policies
- Thorough understanding of risks
- Maintain privilege
- Watch for retaliation

### Investigation Don'ts
- Don't draw conclusions too early
- Don't ignore potential conflicts of interest
- Don't tell witnesses what others had to say
- Don't reveal the facts
- Don't let time go by before writing interview notes

### Potential Pitfalls
- Negligent hiring/retention
- Negligent investigation
- Inability to separate facts from innuendos
- Poor documentation
- Incurring additional liability
Investigations & Corrective Action

Play 8: Conduct Investigations – Communications

With an ongoing investigation, communication should be held between the following interested parties, as appropriate:

- Special Counsel and Forensic Accountants (collectively, the “Investigators”)  
- Audit Committee  
- External Auditors  
- Management (as appropriate)  
- Regulators  
- Investor
Investigations & Corrective Action

Play 8: Conduct Investigations – Obtaining the Facts

The investigation team needs to learn the facts in an independent fashion.

1. Documents
   - Attorneys should issue a document retention notice including instructions to stop any routine document destruction policies.
   - Should be reviewed prior to interviews if possible, but must balance volume of documents with need to initiate interviews.
   - Remember: the documents may not be legitimate.

2. Electronic Evidence
   - Determine all sources of electronic evidence (desktops, laptops, servers, mobile devices, USB sticks/external drives) to forensically image.
   - Maintain chain of custody.

3. Interviews
   - Determine who will conduct the interviews, who will be interviewed, room setup, etc.
   - Obtain content from interviewee for interview and collect written statements.
   - Upjohn Warnings.
   - Prepare Memorandum of Interview.

4. Public Record Searches
   - Collect information regarding other litigation; business and financial affiliations; assets, liabilities and liens; and other personal information.
Investigations & Corrective Action

Play 8: Conduct Investigations – Interview Traps

The following traps should be avoided while conducting an interview:

- Too many closed-ended questions/Not enough open-ended
- Getting personal or judgemental
- Making assumptions
- Not being prepared
- Not setting aside enough time
- Allowing distractions
- Not asking the hard questions

- Interrupting
- Not allowing the interviewee to talk - filling the dead air
- Failure to verify what they have been told during an interview
- Divulging what they know or don’t know
- Poor or non-existent notes
- Acting authoritative
- Not following instincts
Investigations & Corrective Action

Play 8: Conduct Investigations – Interview Notes

- Include context details of the interview such as who, where, and when
- Notes should be taken as the interview is being conducted
- Decide on notes style beforehand (verbatim vs. summary)
- Review notes after interview to clean up any typos and verify all notes make sense
Investigations & Corrective Action

Play 8: Conduct Investigations – Report Findings

Report format is a **client decision**, (written vs. verbal)

- If done properly, report will remain privileged unless company waives privilege
- **Memorializes** the process
- May disclose to government to show cooperation
- Courts have found it **difficult to assess** whether a thorough investigation was conducted **without a written report**

Report content should include

- Background and Summary of the **allegation**
- The **scope** of the investigation
- A **detailed description** of the process utilized to conduct the investigation
- The **factual findings**
- What **limitations** were involved and why
- Recommendations (optional)
- Exhibits
Monitoring Activities

Play 9: Monitor Your Progress

Organizations and risk landscapes are dynamic and always evolving. This means that implementing an effective fraud risk management program requires ongoing monitoring to stay on top of those changes, and get ahead of emerging threats.

Monitoring almost always comes last when organizations build FRM programs, sometimes even as an afterthought. However, monitoring and periodic evaluations provide vital insight into the effectiveness of fraud risk management activities and help identify areas for improvement.

Tips

1. **Focus on the effectiveness.**
   This means you should focus on measuring outcomes instead of outputs.

2. **Use the results to improve.**
   Conducting monitoring and evaluation activities is the first step. Ensuring that there are mechanisms in place to track progress on corrective actions is key to closing identified gaps.
Monitoring Activities
Play 9: Monitor Your Progress – Monitor and Evaluate

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.

**Monitoring Activities**

- The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

- The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
Monitoring Activities
Play 10: Report on Your Progress

Communicating the results and outcomes of your fraud risk management program at all levels of your organization—and to your organization’s leadership—is essential to **increase awareness, showcase accomplishments, and motivate senior leaders to prioritize FRM efforts**.

You should be communicating along the way, but it is important to have periodic reporting to share outcomes, insights and lessons learned. The information you include is up to you – just be sure you consider all your fraud risk management activities.
The Anti-Fraud Playbook outlines a number of supplemental tools you can leverage to apply the best practices and guidance outlines. This includes:

**Anti-Fraud Playbook**
- Enterprise Anti-Fraud Maturity Assessment Model
- Fraud Risk Map Template

**ACFE’s Fraud Risk Tools**
- Interactive Scorecards
- Library of Anti-Fraud Data Analytics Tests
- Risk Assessment & Follow-Up Action Templates
- Points of Focus Documentation

Any final questions?
Speakers

James Ruotolo
Senior Manager
Fraud Risk Mitigation & Analytics
Grant Thornton
James.Ruotolo@us.gt.com
@jduotolo

Holly Johnson
Senior Manager
Forensic Advisory Services
Grant Thornton
Holly.Johnson@us.gt.com
Disclaimer

This Grant Thornton LLP presentation is not a comprehensive analysis of the subject matters covered and may include proposed guidance that is subject to change before it is issued in final form. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at conclusions that comply with matters addressed in this presentation. The views and interpretations expressed in the presentation are those of the presenters and the presentation is not intended to provide accounting or other advice or guidance with respect to the matters covered.

For additional information on matters covered in this presentation, contact your Grant Thornton LLP adviser.
Disclaimer

IRS Circular 230 disclosure: To ensure compliance with requirements imposed by the U.S. Internal Revenue Service, we inform you that any U.S. federal tax advice contained in this PowerPoint is not intended or written to be used, and cannot be used, for the purpose of (a) avoiding penalties under the U.S. Internal Revenue Code or (b) promoting, marketing or recommending to another party any transaction or matter addressed herein.

The foregoing slides and any materials accompanying them are educational materials prepared by Grant Thornton LLP and are not intended as advice directed at any particular party or to a client-specific fact pattern. The information contained in this presentation provides background information about certain legal and accounting issues and should not be regarded as rendering legal or accounting advice to any person or entity. As such, the information is not privileged and does not create an attorney-client relationship or accountant-client relationship with you. You should not act, or refrain from acting, based upon any information so provided. In addition, the information contained in this presentation is not specific to any particular case or situation and may not reflect the most current legal developments, verdicts or settlements.

You may contact us or an independent tax advisor to discuss the potential application of these issues to your particular situation. In the event that you have questions about and want to seek legal or professional advice concerning your particular situation in light of the matters discussed in the presentation, please contact us so that we can discuss the necessary steps to form a professional-client relationship if that is warranted. Nothing herein shall be construed as imposing a limitation on any person from disclosing the tax treatment or tax structure of any matter addressed herein.

© 2018 Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd. All rights reserved. Printed in the U.S. This material is the work of Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd.
Thank you for attending

www.grantthornton.com
twitter.com/GrantThorntonUS
linkd.in/GrantThorntonUS