

The Importance of Fraud Risk Management

January 22, 2026



Speakers



DJ Rossini
Managing Director
Risk Advisory Services

D +1 312 602 8830
E dj.rossini@us.gt.com

Learning Objectives

1

Why is Fraud Risk Management important?

- How organizations are at risk from fraud – financial and non-financial factors

2

Overview of a Fraud Risk Management program

- Describe the components of a fraud risk management program
- Discuss the concept of maturity as it relates to a fraud risk management program

3

Practical Strategies to safeguard against fraud

- Discuss several easy-to-implement solutions that can help manage fraud risk.
- Describe how corporate counsel can and should be involved in fraud risk management.

Why is Fraud Risk Management Important?

Financial Impact



Occupational Fraud 2024: A Report to the Nations – Association of Certified Fraud Examiners

Why is Fraud Risk Management Important?

Non-Financial Impact



Reputational Damage

Fraud can severely harm an organization's reputation, leading to a loss of trust among customers, clients, and stakeholders.



Legal and Regulatory

Even if financial losses are immaterial, resulting litigation or regulatory actions can be costly and divert company resources.

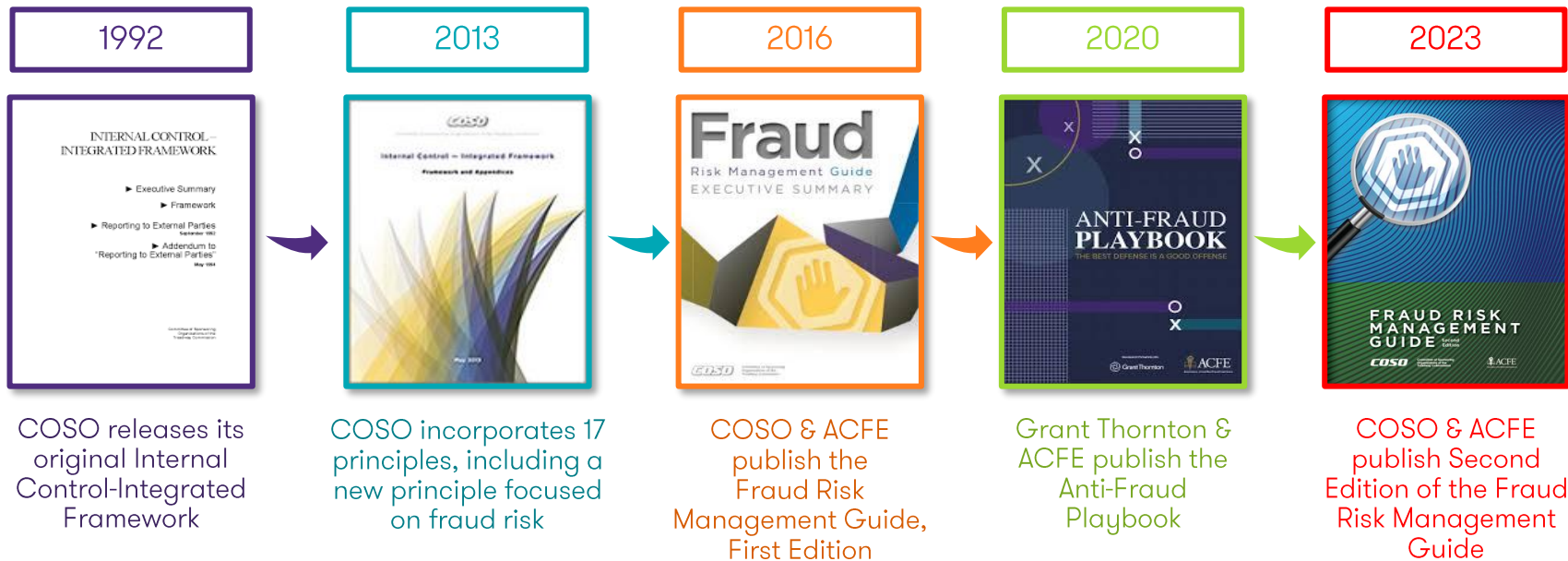


Increased Scrutiny

Organizations that experience fraud may face increased scrutiny from regulators, auditors, and stakeholders, leading to stringent oversight measures.

Proactively Approaching Fraud

The Best Defense is a Good Offense

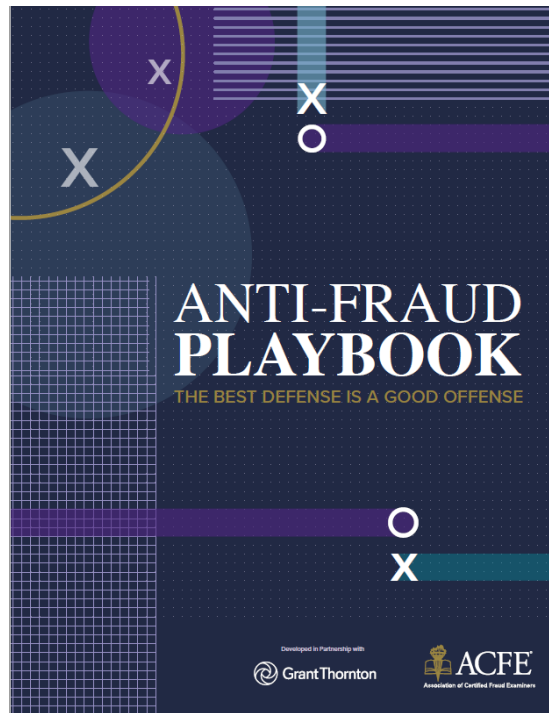


The Anti-Fraud Playbook

A Proactive Approach to Fraud Risk

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 an organization's FRM program** and ultimately facilitate effective and proactive FRM.



Grant Thornton / ACFE
Anti-Fraud Playbook

COSO's Fraud Risk Management Principles



Control Environment: The organization establishes and communicates a Fraud Risk Management program



Risk Assessment: The organization performs comprehensive fraud risk assessment



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



Information and Communication: The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective actions



Monitoring Activities: The organization selects, develops, and performs ongoing evaluations

The Anti-Fraud Playbook

The Phases & Plays



Fraud Risk Governance

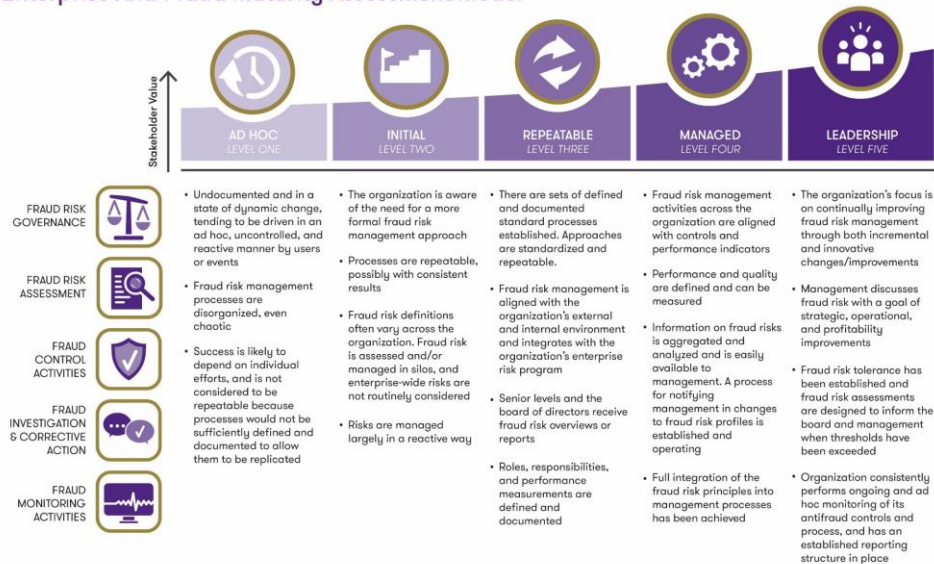
Play 1: Understand where you are & where you want to be

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.

Enterprise Anti-Fraud Maturity Assessment Model®

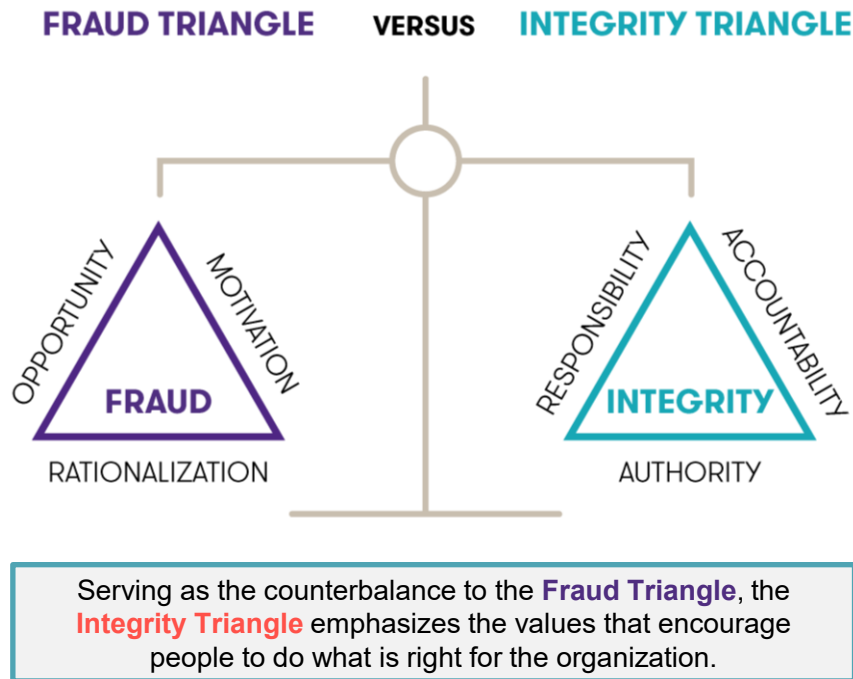


Fraud Risk Governance

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.



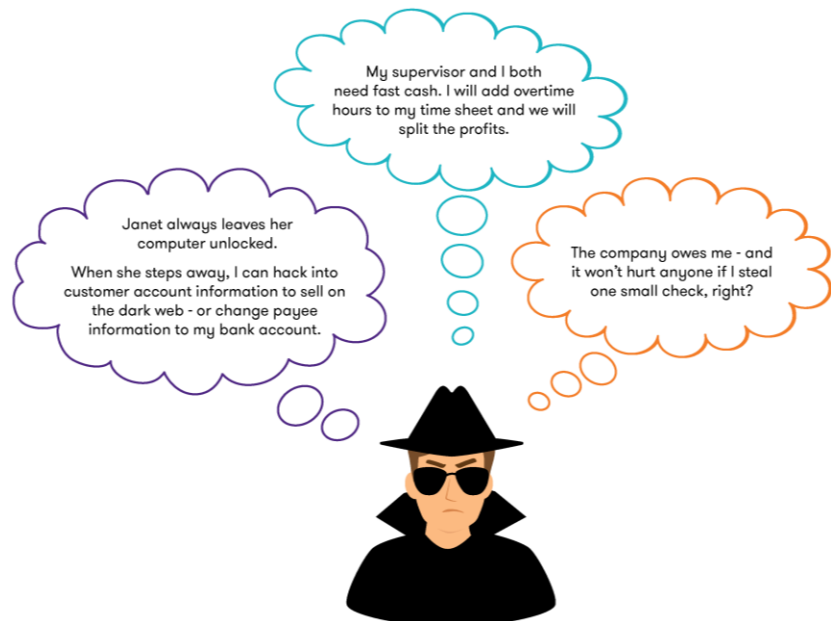
Fraud Risk Assessment

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

	Asset Misappropriation	Financial Misstatement	Corruption
Perpetrator	<ul style="list-style-type: none"> - Any employee - Sole actor or collaborators 	<ul style="list-style-type: none"> - Management & financial reporting - Collusion required 	<ul style="list-style-type: none"> - Procurement, supply chain, inventory control, sales - Individual employee - External party
Scale	Small \$ to Millions	Millions to Billions	Small to Midsize \$
Rewards	<ul style="list-style-type: none"> - Cash enrichment - Inventory or Fixed Assets - Employee resources 	<ul style="list-style-type: none"> - Performance bonuses - Promotions - Attract new investors - Build brand perception 	<ul style="list-style-type: none"> - Cash enrichment - Gift or trips
Goals	<ul style="list-style-type: none"> - Enrich Employee 	<ul style="list-style-type: none"> - Manipulate actual results - Falsify existence of events - Suppress existence of actual events 	<ul style="list-style-type: none"> - Provide preferential status to certain vendor(s) - Allow for monopolistic supplier or price inflation - Enrich employee

Fraud Risk Assessment

Play 4: Discover what you don't know

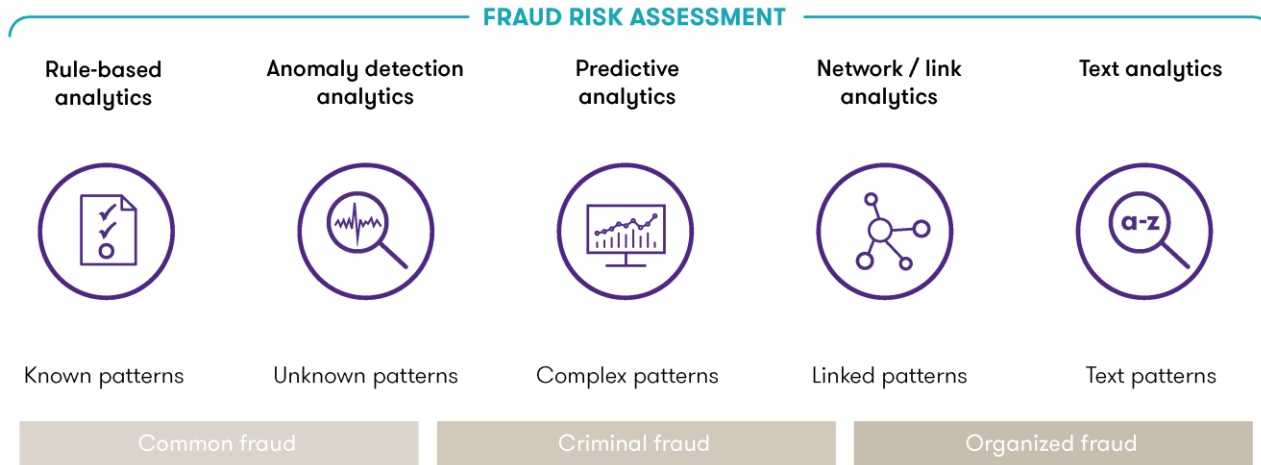
Conducting a fraud risk assessment helps you **understand exactly where your processes may be vulnerable to fraud** and allows for a holistic and detailed look at the fraud risks across the organization.

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**.



Fraud Control Activities

Play 5: Use data to uncover fraud



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.

Fraud Control Activities

Play 6: Knowledge is power

Operational issues	Cultural issues	Financial reporting
<ul style="list-style-type: none"> Weak internal control environment Lack of account reconciliations Customer billing and payment complaints Numerous credit memos issued to clients of one sales representative Vendor name consists of initials or vague business purpose Excessive "void", missing or destroyed checks Unsecured signature stamp or electronic signatures 	<ul style="list-style-type: none"> Employees living beyond their means Family members of leadership employed by the organization Frequent turnover of accounting personnel Management compensation depends on meeting quantified targets Organization has engaged in opinion shopping Large number of related party relationships Poor tone at the top 	<ul style="list-style-type: none"> Increasing A/R compared to cash Flat or declining sales with increasing cost of sales Increasing "soft" expenses (like "temporary labor", "consulting", "advertising") "Eternal" reconciling items Organization undergoes frequent structural re-organizations Organization always meets revenue projections Organization often reports financial results "at the last minute" or late

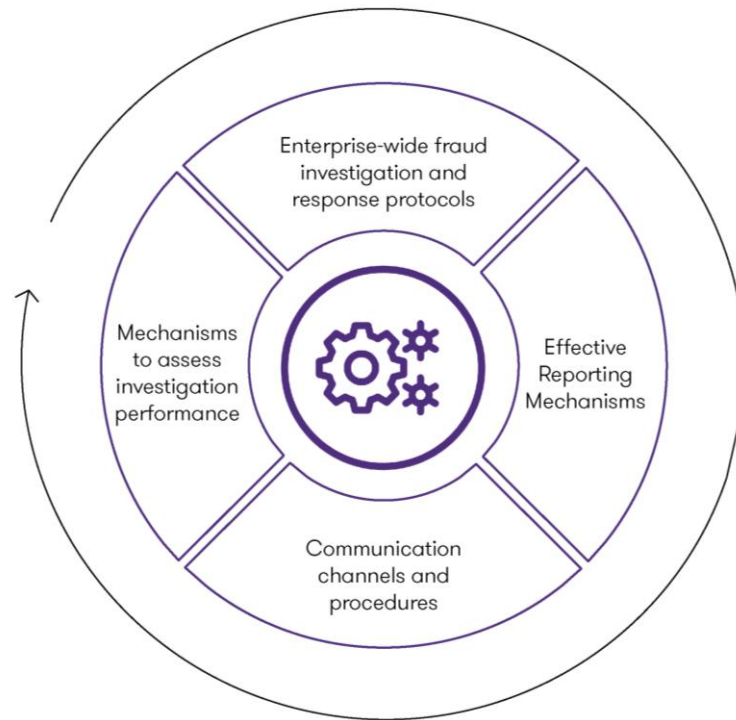
Investigations & Corrective Action

Play 7: Lay the groundwork for investigations

An effective fraud risk management framework includes 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.**

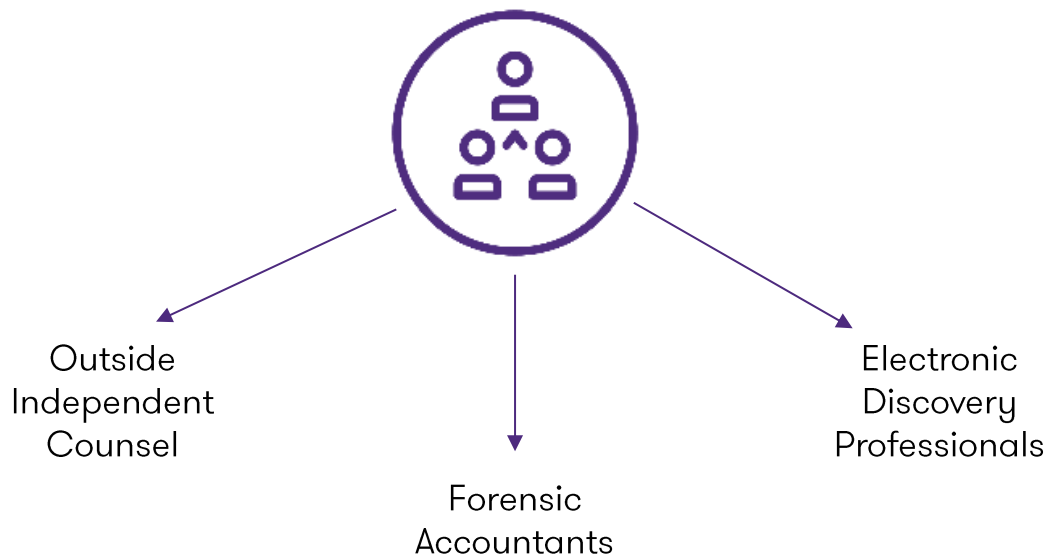
A **necessary first step** is to **lay the proper foundations** for such an investigation by adopting the proper tools and mechanisms to evaluate, communicate, and remediate both instances of potential fraud and the control deficiencies that lead to fraud.

This will **empower your organization to prioritize, assign, and monitor reported fraud** and implement effective corrective actions.



Investigations & Corrective Action

Play 7: Lay the groundwork for investigations



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 will typically include the following components:

Computer forensics

E-discovery

Data analytics
(i.e., predictive coding)

Digital forensics

Records and risk management

Incident response

Data breach investigations

The investigation will involve different steps depending on the kind of allegation, but below are some general factors to consider:

Time sensitivity

Confidentiality

Legal privileges

Objectivity

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 advisor 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.

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

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



Focus on the effectiveness.

This means you should focus on measuring outcomes instead of outputs.



Use the results to improve.

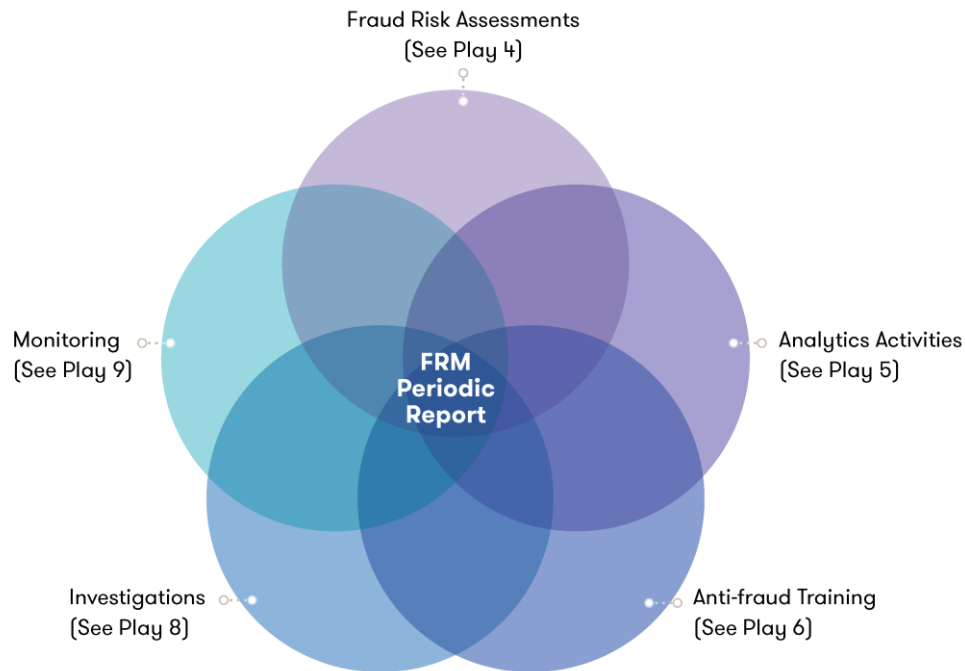
Conducting monitoring and evaluation activities is the first step. Ensuring that there are mechanisms in place to track progress on corrective actions is key to closing identified gaps.

Monitoring Activities

Play 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.



Easy-to-Implement Solutions - Hotline

Whistleblower hotlines are one of the easiest and most effective fraud detection mechanisms. Hotlines:

- **Encourage reporting** by providing a safe and anonymous way for employees to report unethical behavior or fraud, which might otherwise go unreported due to fear of retaliation.
- **Allow for early detection**, catching fraud cases before they escalate into more significant problems, **allowing the organization to address fraud allegations promptly and mitigate potential damage**.
- **Promote ethical culture** by demonstrating the organization's commitment to transparency and ethical behavior, **fostering a culture of integrity and accountability**.
- **Help ensure compliance with legal and regulatory requirements**, reducing the risk of fines, penalties and legal action.

Occupational Fraud 2024: A Report to the Nations – Association of Certified Fraud Examiners

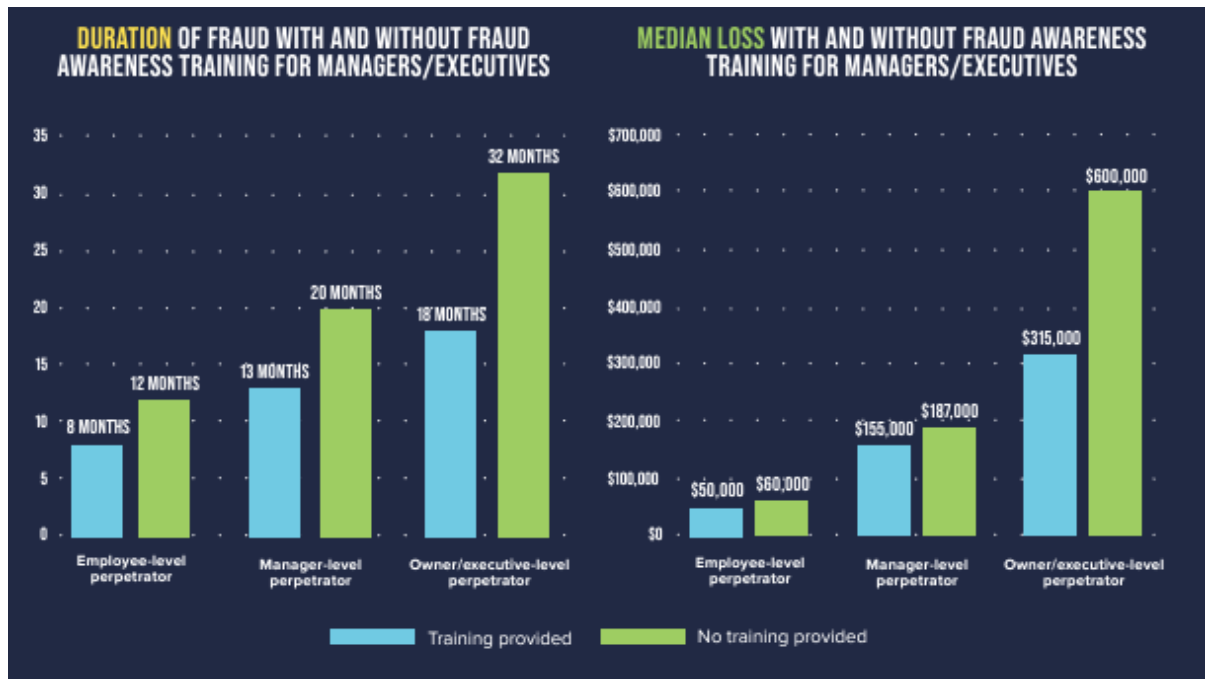


Easy-to-Implement Solutions - Training



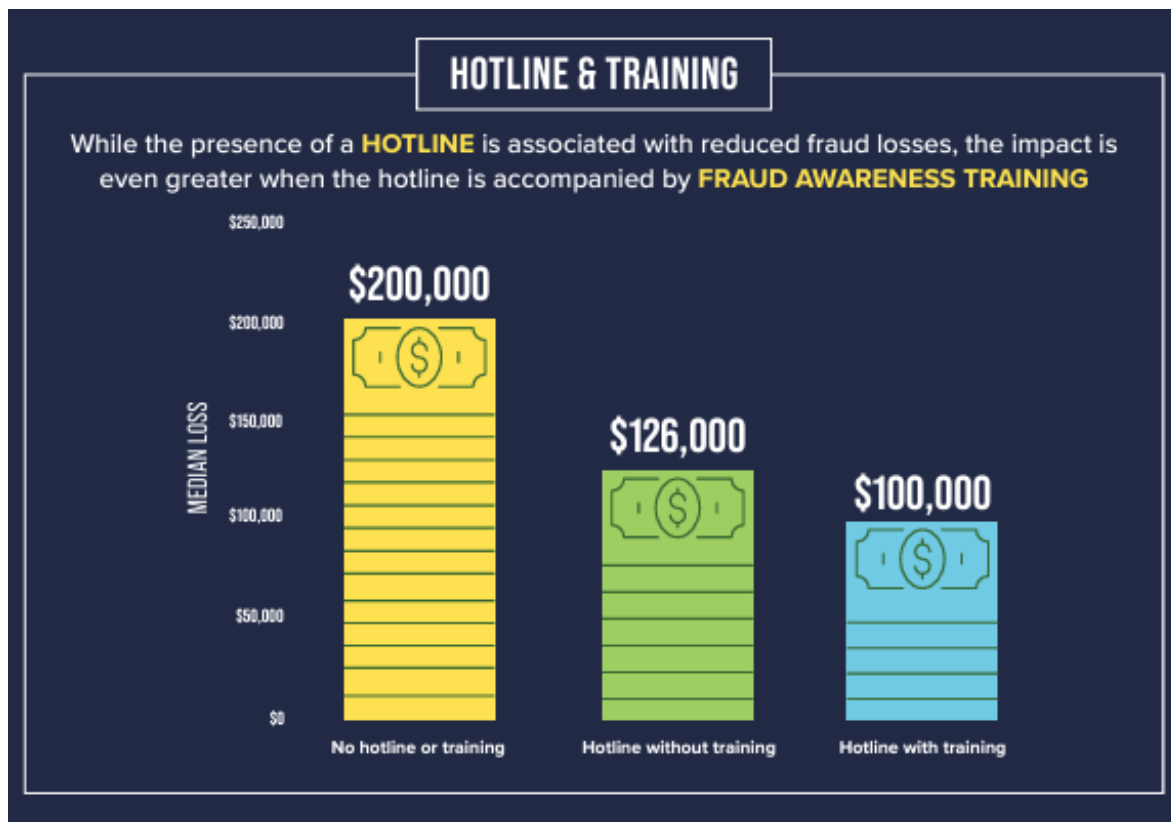
Occupational Fraud 2024: A Report to the Nations – Association of Certified Fraud Examiners

Easy-to-Implement Solutions - Training



Occupational Fraud 2024: A Report to the Nations – Association of Certified Fraud Examiners

Easy-to-Implement Solutions - Training

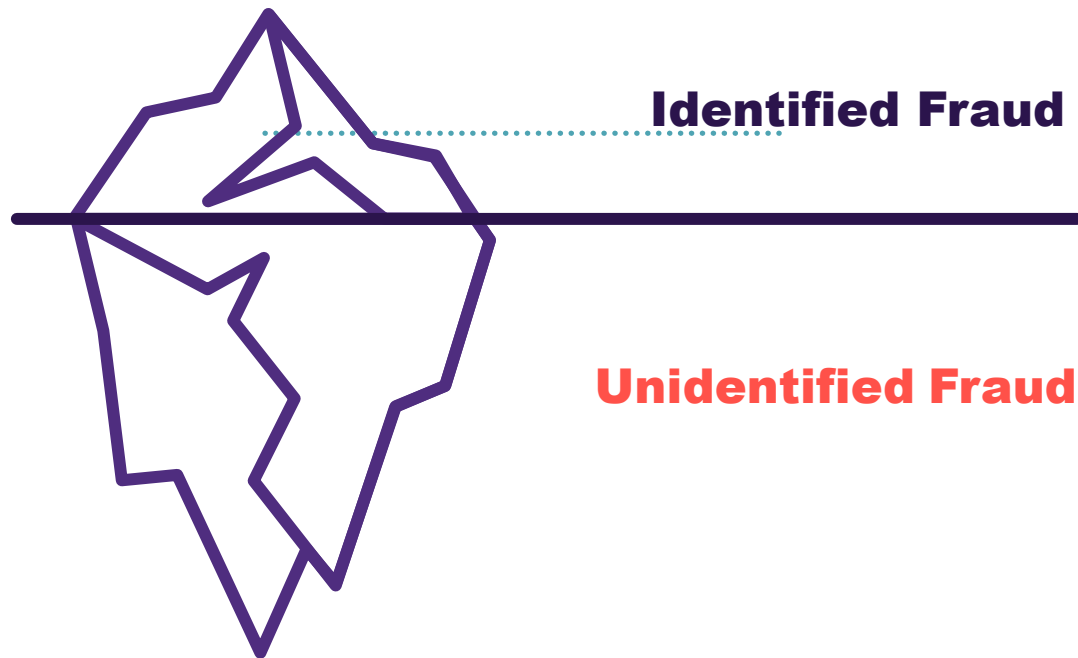


Occupational Fraud 2024: A Report to the Nations – Association of Certified Fraud Examiners




The Cost of Fraud

Fraud is like the proverbial iceberg; the deceptive nature of fraud means that it is unknown until discovered, leading to potential 'submerged' or unknown frauds beneath the surface.

According to the Association of Certified Fraud Examiners (ACFE), CFEs estimate that organizations around the world lose an estimated **5%** of their annual revenues to fraud. Applied the 2021 Gross World Product (GWP), this amounts to **\$4.7 trillion** in potential global fraud losses.



Types of Fraud Risk

Fraud Type	 External Fraud	 Internal Fraud	 Individual Fraud
Definition	<p>Committed by outside organizations, typically by individuals or groups, against organizations.</p>	<p><i>Aka "Occupational Fraud"</i> the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organization's resources or assets</p>	<p>Devised schemes and actions designed to defraud individuals</p>
Examples	<p>Intellectual Property Theft Insurance Fraud Hacking / Ransomware False Billing Schemes</p>	<p>Corruption Asset Missappropriation Financial Statement Fraud</p>	<p>Identity Theft Ponzi Schemes Phishing Schemes Advanced-Fee Frauds</p>

Questions?



DJ Rossini
Managing Director
Risk Advisory Services

D +1 312 602 8830
E dj.rossini@us.gt.com



"Grant Thornton" refers to the brand name under which the Grant Thornton member firms provide services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton LLP and Grant Thornton Advisors LLC (and their respective subsidiary entities) practice as an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations and professional standards. Grant Thornton LLP is a licensed independent CPA firm that provides attest services to its clients, and Grant Thornton Advisors LLC and its subsidiary entities provide tax and business consulting services to their clients. Grant Thornton Advisors LLC and its subsidiary entities are not licensed CPA firms.

Grant Thornton International Limited (GTIL) and the member firms, including Grant Thornton LLP and Grant Thornton Advisors LLC, are not a worldwide partnership. GTIL and each member firm are separate legal entities. Services are delivered by the member firms; GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

© 2024 Grant Thornton Advisors LLC | All rights reserved | U.S. member firm of Grant Thornton International Ltd.