



# Anti-Fraud Playbook

The best defense is a good offense

- 
- **September 7, 2020**
  - **11:00 am CST**



# Speakers



**James Ruotolo**  
Senior Manager  
Fraud Risk Mitigation  
**T** +1 203 327 8337  
**E** james.ruotolo@us.gt.com



**Sophia Carlton**  
Manager  
Fraud Risk Mitigation  
**T** +1 703 637 2614  
**E** sophia.carlton@us.gt.com

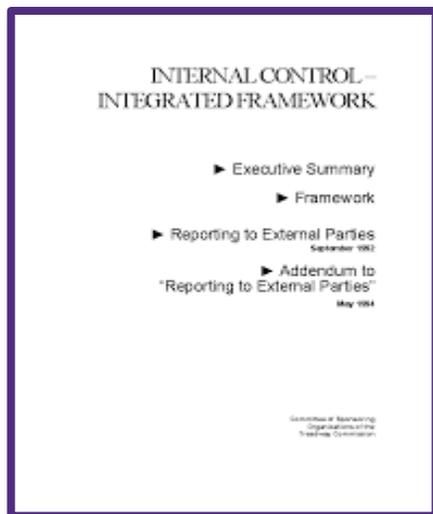
# What We Will Cover



- 1 Introduction**
- 2 The Phases & Plays**
- 3 Q&A**

# How Did We Get Here?

**1992**



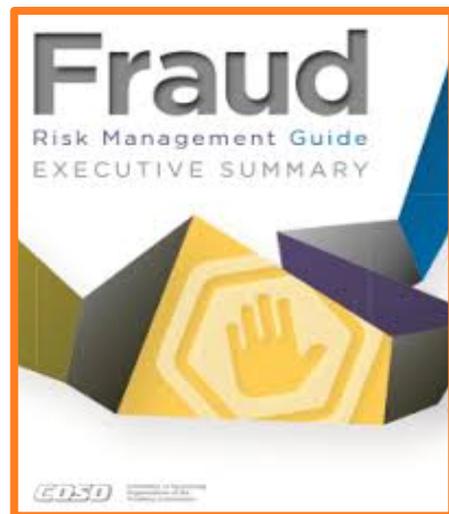
**COSO releases its original Internal Control-Integrated Framework**

**2013**



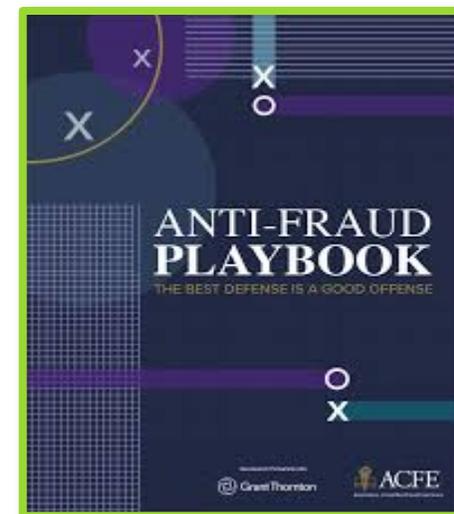
**COSO incorporates 17 principles, including a new principle focused on fraud risk**

**2016**



**COSO & ACFE publish the Fraud Risk Management Guide**

**2020**



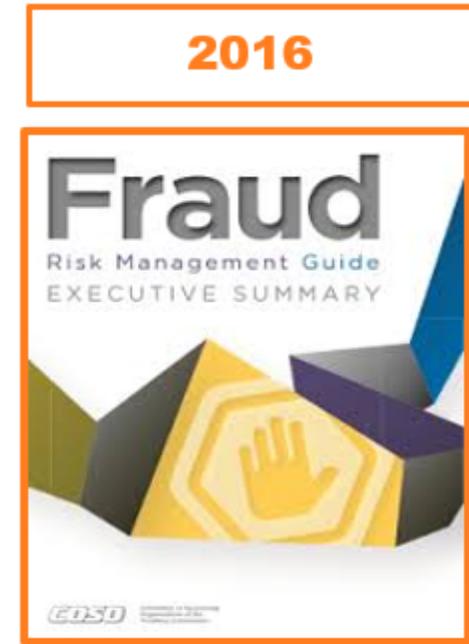
**Grant Thornton & ACFE publish the Anti-Fraud Playbook**

# COSO's Fraud Risk Management Guide



The Guide calls for the development of an antifraud governance structure, a formal fraud risk assessment, the development of antifraud controls and a monitoring plan.

The Guide is intended to be supportive of and consistent with the 2013 Framework and can serve as best practices and guidance for organizations to follow in addressing Principle 8.



**COSO & ACFE  
publish the  
Fraud Risk  
Management Guide**

# 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



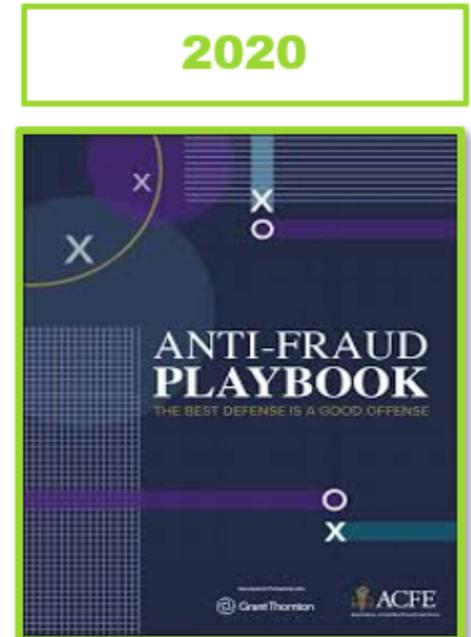
**Fraud Risk Management Monitoring Activities:** The organization selects, develops, and performs ongoing evaluations



# 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.**



**Grant Thornton & ACFE publish the Anti-Fraud Playbook**

---

# 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

## Fraud Risk Assessment

Play #3 – Think Like a Fraudster

Play #4 – Discover What You Don't Know

## Investigations and Corrective Action

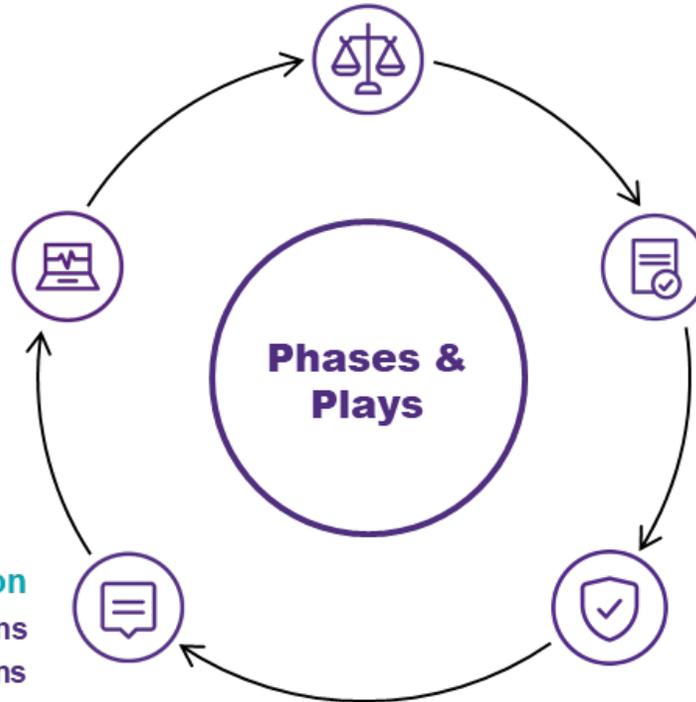
Play #7 – Lay the Groundwork for Investigations

Play #8 – Conduct Investigations

## Fraud Control Activities

Play #5 – Use Data to Uncover Fraud

Play #6 – Knowledge is Power





# Fraud Risk Governance

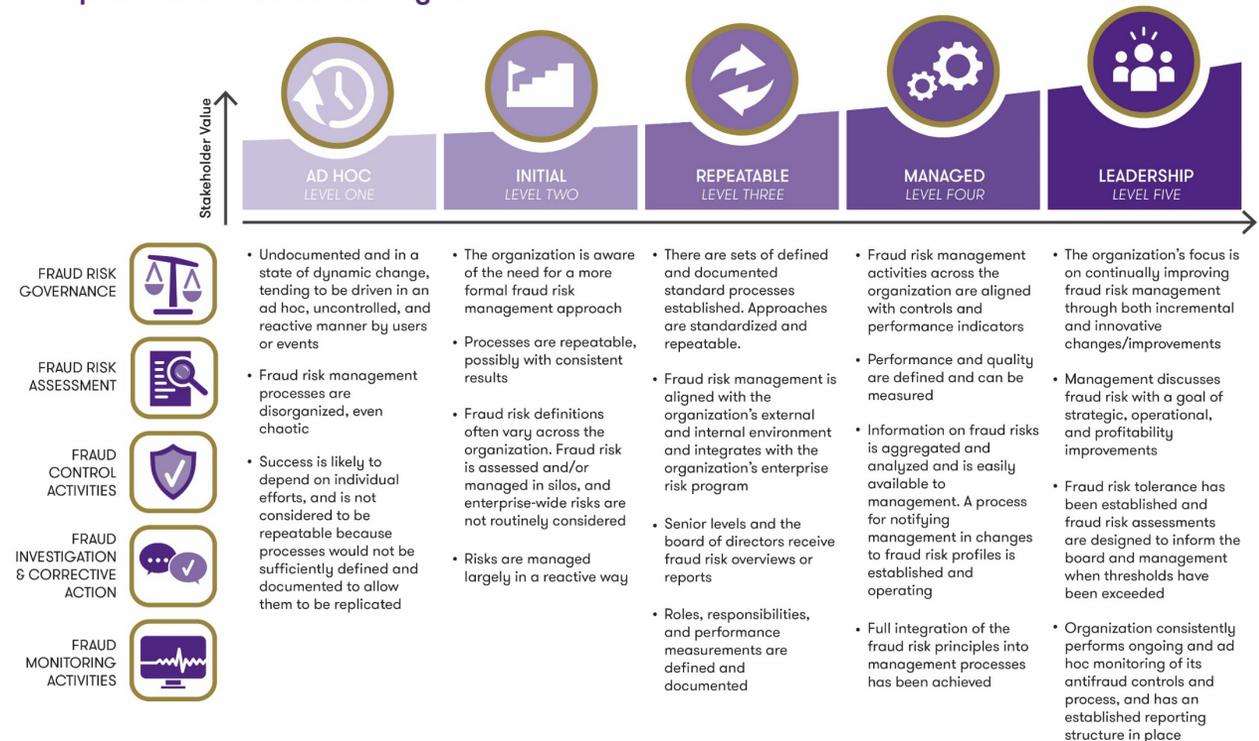
## Play 1: Understand Where You Are & Where You Want to Be

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<sup>®</sup>





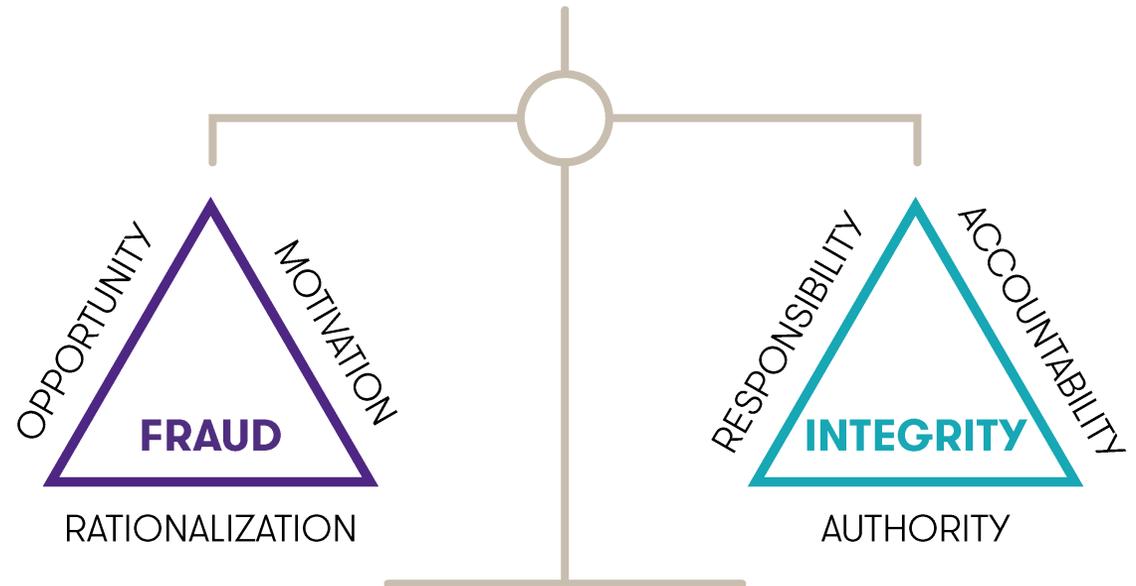
# Fraud Risk Governance

## 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 TRIANGLE VERSUS INTEGRITY TRIANGLE



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.

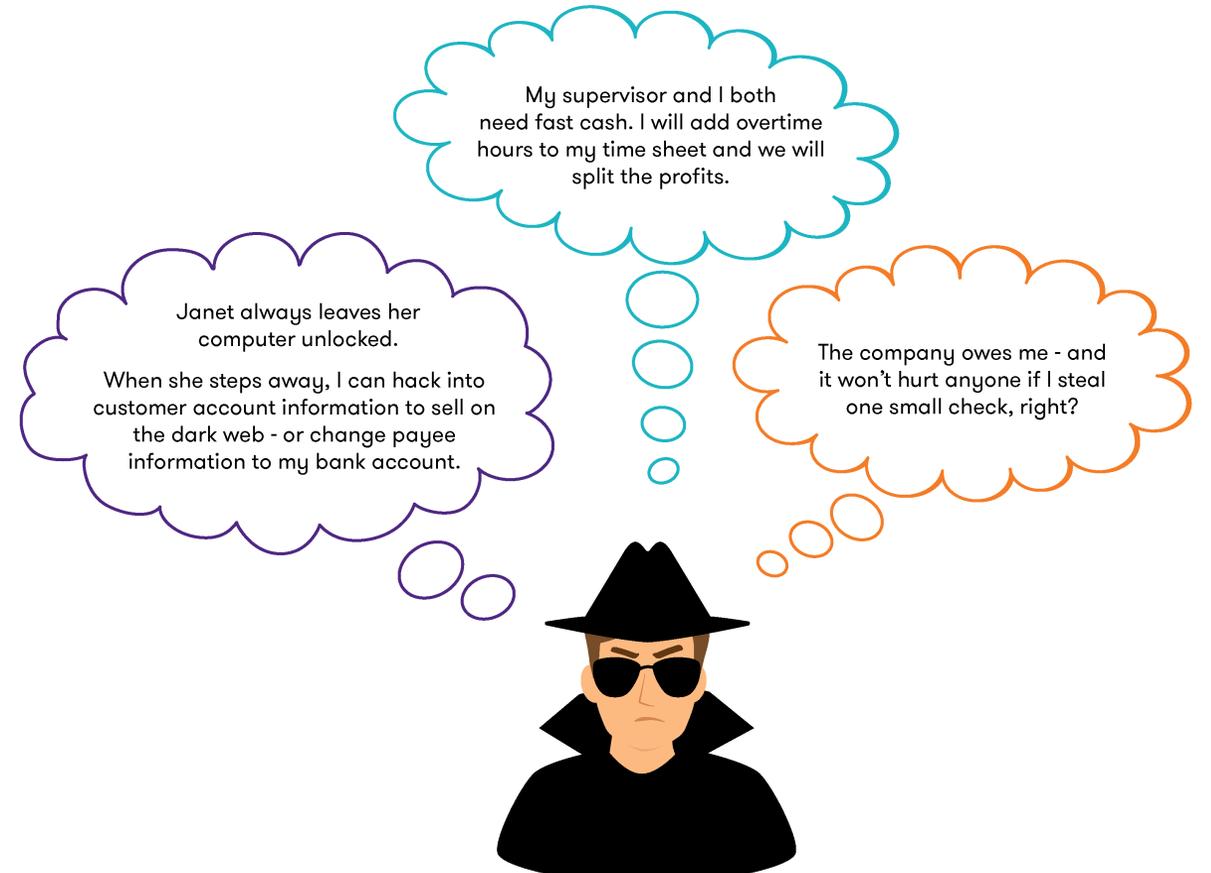
# Fraud Risk Assessment

## 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.



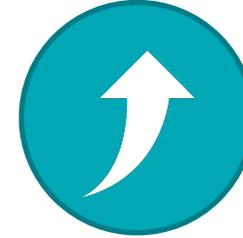
# Fraud Risk Assessment

## Play 3: Think Like a Fraudster



**At a minimum, a Fraud Risk Map should include information for:**

- Related Unit of Analysis (i.e., Department Name or Business Unit)
- Actor
- Fraud Risk Entry Point (or Channel)
- Fraud Scheme



**It can include a number of additional elements, such as:**

- Fraud Category
- Fraud Type
- Related Controls
- Internal vs. External
- Identified Control Gaps or Weaknesses



# Fraud Risk Assessment

## Play 3: Think Like a Fraudster

### Key considerations when developing your fraud risk map include:

-  We recommend organizing your Fraud Risk Map by your **preferred unit of analysis** to ensure your Fraud Risk Map aligns to your Fraud Risk Assessment.  
  
When identifying fraud schemes, we recommend doing so in a **group setting**.
-  Consider **both the actor** (i.e., the perpetrator) and **the fraud risk entry points** (i.e., the function or process which the actor capitalizes on to carry out the fraud scheme).
-  Remember that **not all fraud is financial**. Some fraud can affect an organization's reputation even if it doesn't lead to major financial loss.
-  **Leverage available resources** - including existing risk registers at your organization, along with industry emerging trends and research - **to ensure your listing is comprehensive**.

Business Unit	Internal or External	General Fraud Category	Fraud Scheme Type	Fraud Scheme	Sub-Fraud Scheme	Actor	Fraud Risk Entry Point	Underlying Fraud Risk	Related Control Activities
Payroll	Internal	Asset Misappropriation	Fraudulent Disbursements	Payroll	Overpayment	Payroll Employee / Management	Payroll Records	A payroll employee or member of management submits an unauthorized pay rate increase, either for themselves or another internal party/accomplice.	<ul style="list-style-type: none"> <li>Any change to an employee's salary requires more than one level of approval</li> </ul>
Payroll	Internal	Asset Misappropriation	Fraudulent Disbursements	Payroll	Ghost Employee	Payroll Employee / Management	Payroll Records	A payroll employee or member of management creates a fake employee in the payroll records and falsifies the payment record so that the direct deposit information is replaced with bank account information of his/her own.	<ul style="list-style-type: none"> <li>Payroll list is periodically reviewed for duplicate or missing Social Security Numbers (SSNs), home addresses or telephone numbers</li> <li>Appropriate forms are completed and signed by the employee to authorize payroll deduction and withholding exemptions</li> </ul>
All (Any unit in which employees may submit expenses for reimbursement)	Internal	Asset Misappropriation	Fraudulent Disbursements	Expense Reimbursement	Mischaracterized Expenses	Employee / Management	Expense Reimbursement	An employee or member of management submits an expense reimbursement for a personal expense, claiming the expense was business related.	<ul style="list-style-type: none"> <li>Employees are required to submit detailed expense reports containing receipts, explanations, amounts, etc.</li> <li>Supervisors are required to review and approve all reimbursement requests</li> </ul>
All (Any unit in which employees may submit expenses for reimbursement)	Internal	Asset Misappropriation	Fraudulent Disbursements	Expense Reimbursement	Overstated Expenses	Employee / Management	Expense Reimbursement	An employee or member of management submits an expense reimbursement for a legitimate business expense, but overstates the cost of the expense to fraudulently increase the reimbursement.	<ul style="list-style-type: none"> <li>Spending limits are in place to limit expenses on hotels, meals, etc.</li> <li>Supervisors are required to review and approve all reimbursement requests</li> </ul>



# Fraud Risk Assessment

## Play 3: Think Like a Fraudster

### Checklist



**Determine how you want to break out your fraud risk map.** This can be by department, business function, etc.



**Integrate all the identified fraud schemes into a comprehensive fraud risk map** for your organization.



**Develop your fraud risk map framework** in line with how you want to break out your fraud risk map as determined in the previous step.



**Periodically refresh and iterate the fraud risk map** as part of your ongoing FRM and fraud risk assessment activities.



**Identify internal and external fraud schemes for each area of your fraud risk map.** For example, if you chose to break it out by department, then do this for each department.





# Fraud Risk Assessment

## Play 4: Discover What You Don't Know

**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?



# Fraud Risk Assessment

## Play 4: Discover What You Don't Know

In order to garner the most actionable information and obtain the most efficient use of stakeholder time, it's important to understand when to use each technique.

### Interviews

Appropriate for senior management or when you need to solicit input in a targeted session

### Surveys

Appropriate in early stages of risk assessment and are then followed on by interviews or workshops for deeper analysis

### Workshops

Appropriate when gathering a cross-functional groups to break down silos and discuss how process and risks interrelate

**Tip:** A mature risk assessment process should employ multiple techniques.



**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

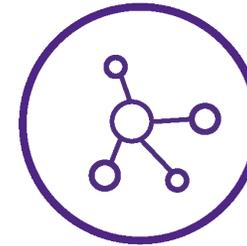
Rule-based analytics

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

# 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.



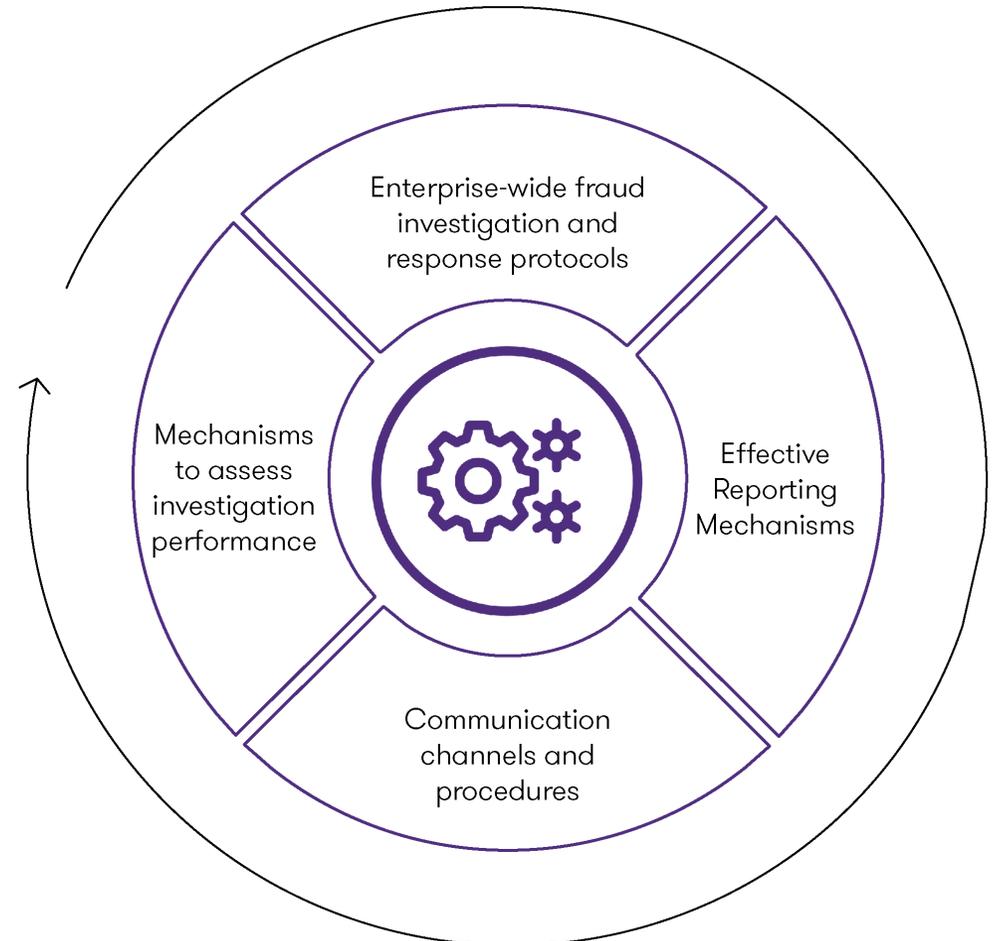
# Investigations & Corrective Action

## Play 7: Lay the Groundwork for Investigations

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.





# 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

# Monitoring Activities

## Play 9: Monitor Your Progress



### 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.

**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.

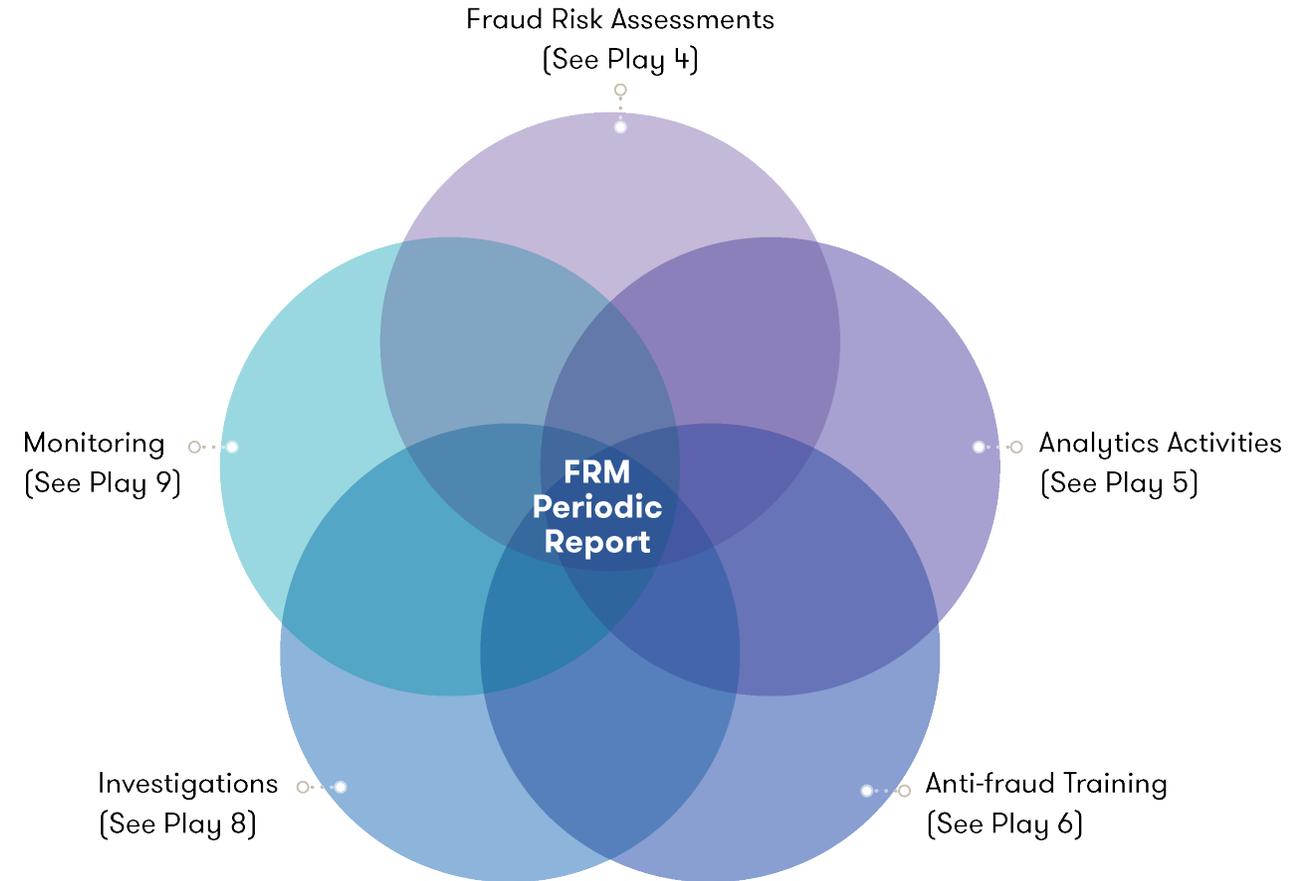


# Monitoring Activities

## 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.





# Supplemental Tools

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

<https://www.acfe.com/fraudrisktools-tools.aspx>

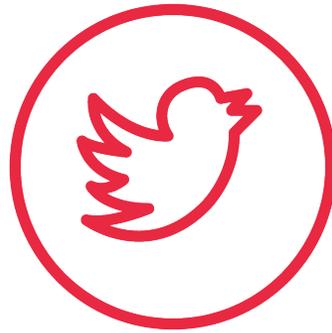
# Any final questions?



# Thank you for attending



[www.grantthornton.com](http://www.grantthornton.com)



[twitter.com/GrantThorntonUS](https://twitter.com/GrantThorntonUS)



[linkd.in/GrantThorntonUS](https://linkd.in/GrantThorntonUS)

# 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.