ANTI-FRAUD PLAYBOOK

THE BEST DEFENSE IS A GOOD OFFENSE

Developed in Partnership with

Grant Thornton

ACFE®

Association of Certified Fraud Examiners

Founded in 1988 by Dr. Joseph T. Wells, CFE, CPA, the ACFE is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with more than 85,000 members in more than 150 countries, the ACFE is reducing business fraud worldwide and providing the training and resources needed to fight fraud more effectively.

The positive effects of anti-fraud training are far-reaching. Clearly, the best way to combat fraud is to educate anyone engaged in fighting fraud on how to effectively prevent, detect and investigate it. By educating, uniting and supporting the global anti-fraud community with the tools to fight fraud more effectively, the ACFE is reducing business fraud worldwide and inspiring public confidence in the integrity and objectivity of the profession. The ACFE offers its members the opportunity for professional certification. The Certified Fraud Examiner (CFE) credential is preferred by businesses and government entities around the world and indicates expertise in fraud prevention and detection.

Certified Fraud Examiners

The ACFE offers its members the opportunity for professional certification with the Certified Fraud Examiner (CFE) credential. The CFE is preferred by businesses and government entities around the world, and indicates expertise in fraud prevention and detection. CFEs are anti-fraud experts who have demonstrated knowledge in four critical areas: Financial Transactions and Fraud Schemes, Law, Investigation, and Fraud Prevention and Deterrence.

Membership

Members of the ACFE include accountants, internal auditors, fraud investigators, law enforcement officers, lawyers, business leaders, risk/compliance professionals, and educators, all of whom have access to expert training, educational tools, and resources. Whether their career is focused exclusively on preventing and detecting fraudulent activities or they just want to learn more about fraud, the ACFE provides the essential tools and resources necessary for anti-fraud professionals to accomplish their objectives.

Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd, one of the world's leading organizations of independent audit, tax and advisory firms. Grant Thornton, which operates more than 50 offices in the United States and operates in more than 135 countries, works with a broad range of dynamic publicly and privately held companies, government agencies, and organizations.

Grant Thornton is a leader in fraud risk management. Our fraud risk professionals are progressive thinkers with a wealth of experience developing robust antifraud programs across a wide range of industries, and across organizations of varying missions and sizes. Our proven fraud risk management solutions are based on proprietary methodologies and we have developed industry-leading benchmarking tools, maturity models and customizable, scalable fraud risk assessment methodologies that can be tailored to address the evolving risk landscape and meet the needs, complexities and goals of an organization. Further, Grant Thornton was instrumental in the development of the fraud risk frameworks used both in government and in the private sector. This insight into leading guidance and our deep pool of expertise provide a rich set of leading practices and insights that we bring to our clients to help them combat fraud, and focus mitigation where it matters most.

With the scale to meet your evolving needs, Grant Thornton specializes in personalizing solutions to help you address today's problems and anticipate tomorrow's challenges.

The Anti-Fraud Playbook:

The Best Defense Is a Good Offense

Fraud is happening at your organization; you just don't know it.

Then again, maybe you do, but you are not sure how pervasive the problem is, where to begin your anti-fraud journey, or how to enhance your current fraud risk management practices. Either way, fraud is big business at organizations across the globe. According to the ACFE 2020 *Report to the Nations*, CFEs estimate that **organizations lose 5% of their revenue to fraud each year**. This playbook is designed to reduce this risk and increase profit. The contents include a five-phased approach with ten plays drawn from best practices and leading guidance. Designed to align with the fraud risk management framework provided by the Association of Certified Fraud Examiners (ACFE) and the Committee of Sponsoring Organizations of the Treadway Commission (COSO), the plays in this playbook provide easy-to-use, actionable guidance to help you fight fraud at your organization.

Combating fraud is an ongoing challenge, but this playbook will help you stay a step ahead.

See the Plays

Visit Appendix

Introduction

Why this playbook was developed

In 1992, COSO released its original *Internal Control—Integrated Framework*. COSO revised this Framework in 2013 to incorporate 17 principles, including a new principle focused specifically on fraud risk. Principle 8, one of the Framework's principles pertaining to risk assessment, states:

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

In 2016, the ACFE and COSO published the Fraud Risk Management Guide (the Guide), which is intended to support and be consistent with the revised Framework. The Guide is designed to serve as best-practice guidance for organizations to follow in addressing this COSO's fraud risk assessment principle.

This playbook is intended to provide practical guidance for organizations looking to begin, advance, or benchmark their fraud risk management (FRM) programs against industry best practices. It draws on insights from the Guide and seeks to clarify and operationalize the concepts put forward in that guidance. As such, this playbook includes key questions, checklists, and insights that will enhance your FRM program and ultimately facilitate proactive FRM at your organization.

For additional resources, see the supplemental FRM tools provided by the ACFE to accompany the Guide.

How the playbook is organized

The playbook includes ten plays, which are organized into five phases based on the Guide's five key FRM principles:

- **Fraud Risk Governance**
  The organization establishes and communicates an FRM 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.
- **Fraud Risk Assessment**
  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.
- **Fraud Control Activities**
  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.
- **Fraud Investigation and Corrective Action**
  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.
- **Fraud Risk Management Monitoring Activities**
  The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of FRM is present and functioning and communicates FRM program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

The playbook also includes several appendices that provide additional information, templates, and tools that you can use to implement the ten plays.

The Plays

FIG. 1 Five-Phased Approach

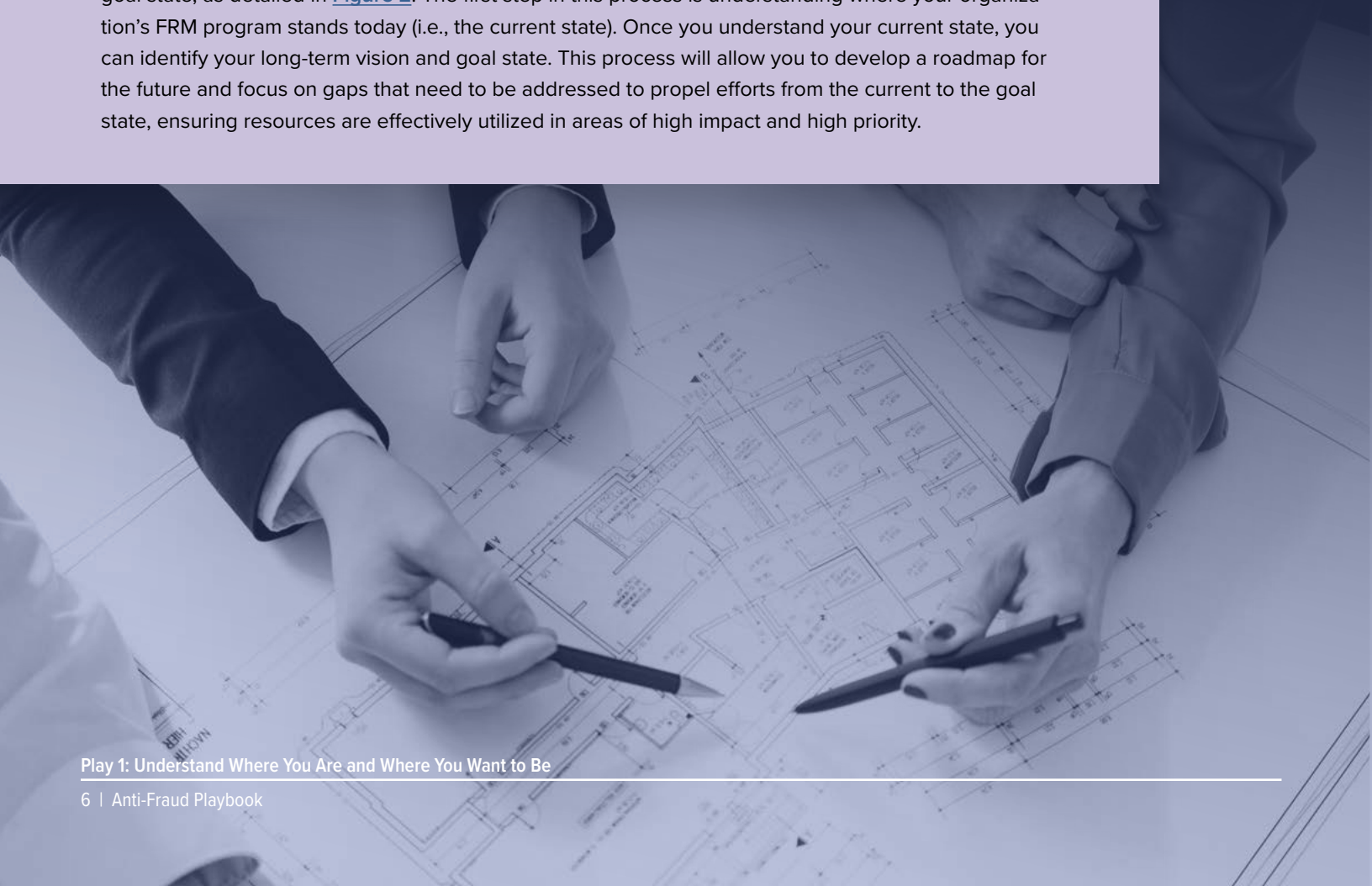
Each phase builds on the previous one, culminating in a robust anti-fraud program.

FRAUD RISK GOVERNANCE

Play 1: Understand Where You Are and Where You Want to Be

The Details

Fraud risk management should be right-sized and tailored for the unique needs of each organization, and not every organization requires the same level of fraud risk management. For example, organizations with limited fraud exposure or those that are willing to accept more fraud risk might not need to aim for the highest level of FRM maturity; instead they might aim for initial or repeatable levels as a goal state, as detailed in Figure 2. The first step in this process is understanding where your organization's FRM program stands today (i.e., the current state). Once you understand your current state, you can identify your long-term vision and goal state. This process will allow you to develop a roadmap for the future and focus on gaps that need to be addressed to propel efforts from the current to the goal state, ensuring resources are effectively utilized in areas of high impact and high priority.



The most effective way to develop your roadmap is by conducting a maturity assessment. The Enterprise Anti-Fraud Maturity Assessment Model© developed by Grant Thornton can be used to assist organizations in identifying where things are—***the current state***—and where things should be—***the goal state***. This model is based on the Guide and can be used to establish the current and goal state of the enterprise's anti-fraud activities in total and across each of the five FRM principles outlined in the Guide.

FIG. 2 Enterprise Anti-Fraud Maturity Assessment Model©

The table below outlines key questions and a checklist to help your organization conduct a maturity assessment and develop a roadmap for the future, in line with the Guide's leading practices and guidance.

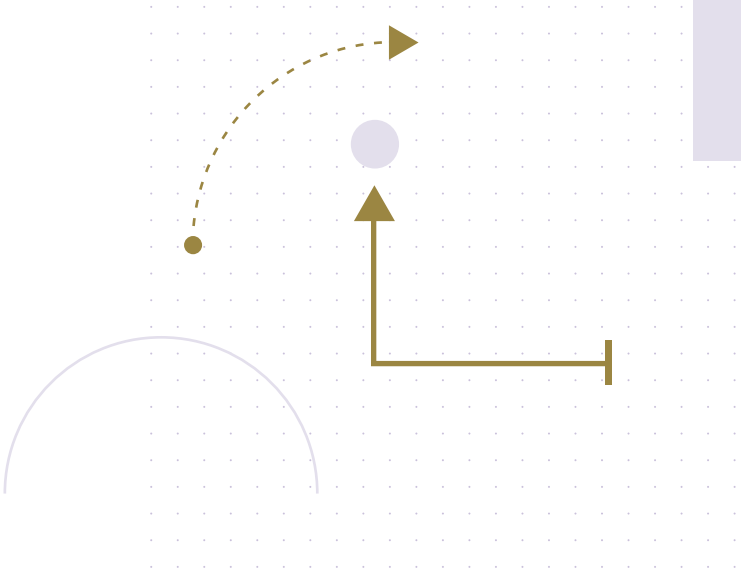
Key questions	Checklist
• Which stage outlined in the maturity model most closely aligns with the current state of your FRM program? » How does this vary across each of the five FRM principles?	☐ **Identify your current state.** Evaluate your organization's current anti-fraud efforts and identify your current state both overall and across each of the five FRM principles. You can leverage the Grant Thornton's Enterprise Anti-Fraud Maturity Assessment Model© and the ACFE's FRM Scorecards to assist in evaluating the current state of your FRM program and related activities (see Tip #1).
• What is the long-term vision for your FRM program? » Which stage outlined in the model most closely aligns with your long-term vision? » How does your long-term vision vary across each of the five FRM principles?	☐ **Identify your goal state.** Identify your organization's goal state both overall and across each of the five FRM principles.
• What do you need to accomplish in both the short- and long-term to achieve your goal state? » What gaps exist between your current state and your goal state? » How will you prioritize FRM efforts and activities related to closing those gaps?	☐ **Develop a comprehensive FRM strategy and roadmap.** Your strategy and roadmap should align to your vision and goal state, including both short- and long-term plans to achieve your goal state based on the gaps identified. You can do this by pinpointing and prioritizing the gaps between your current level of maturity and your goal state both overall and across each of the five FRM principles. For example, the ACFE's FRM Scorecards will highlight where current gaps are across each of the five principles.

TIP #01

The ACFE has developed interactive FRM Scorecards, which can be used to assess the components of your organization's existing FRM program. The scorecards are based on the five FRM principles found in the ACFE/COSO Fraud Risk Management Guide. They support an organization's periodic self-assessment and can be leveraged to easily identify gaps in your current FRM program and to assist in identifying your program's current state.

TIP #02

When establishing a goal state and roadmap for an FRM program, be sure to align the plan with broader organizational objectives. Advanced fraud controls may not be tolerated by the organization if they create excessive complexity or impede core business processes. Strike a balance and be flexible as the needs of the organization evolve over time.



FRAUD RISK GOVERNANCE

Play 2: Create a Culture

The Details

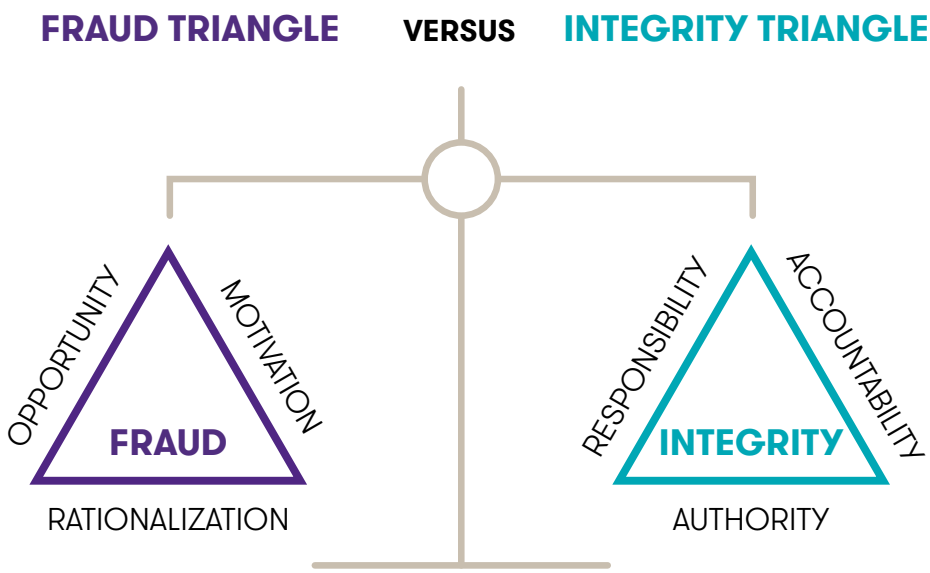
Promoting fraud awareness throughout your organization from the top down is vital to a creating a strong anti-fraud culture, enhancing fraud awareness, and encouraging employees to discuss fraud risks openly and thoughtfully. Fortunately, there are many ways to promote and enhance fraud awareness at your organization, including developing a comprehensive fraud risk governance policy, developing an enterprise-wide anti-fraud training program, hosting fraud awareness events or activities periodically, and communicating roles and responsibilities related to FRM across all levels of the organization. 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.

The key to the success of these efforts is a strong, strategic, and consistent message that can translate fraud awareness into action. ***Enter the Integrity Triangle.*** Serving as the counterbalance to the Fraud Triangle, as shown in Figure 3, the Integrity Triangle emphasizes the values that encourage people to do what is right for the organization. Therefore, no matter where someone is within an organization, this triangle applies to their role—that is, it defines how they do their job.

The three elements of the Integrity Triangle are responsibility, accountability, and authority. When a person understands and appreciates that they have a responsibility to their organization, that they are accountable to its mission, and that they have the authority to effect positive change in that organization, a culture intolerant of improper or inappropriate conduct, such as fraud, is more likely to persist.

The foundation of this concept is awareness. Promoting awareness among your employees about both the threat of fraud and their capacity to combat it is essential for creating an anti-fraud culture and can be a vital tool in fighting fraud in your organization.

FIG. 3 Fraud Triangle Versus Integrity Triangle



The table below outlines the Guide's key points of focus related to fraud risk governance, which highlight important characteristics relating to this principle.[1] You will also find key questions and a checklist that are intended to help your organization achieve a strong anti-fraud culture by establishing a robust anti-fraud governance structure and implementing targeted fraud awareness efforts in line with the Guide's leading practices and guidance.[2]

Points of focus	Key questions
• Makes an organizational commitment to fraud risk management • Supports fraud risk governance • Establishes a comprehensive fraud risk management policy • Establishes fraud risk governance roles and responsibilities throughout the organization • Documents the fraud risk management program • Communicates fraud risk management at all organizational levels	• Do you have a comprehensive FRM policy in place? • Have you established, documented, and communicated roles and responsibilities related to FRM across all levels of the organization, including reporting mechanisms? • Is messaging about fraud risk management communicated throughout your organization, from leadership down to employees at all levels? How do you assess the effectiveness of these efforts? • Do you have fraud awareness initiatives in place? How often are fraud topics discussed throughout all levels of your organization and across key stakeholders?

[1] The ACFE developed Points of Focus Documentation Templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring. You can download these templates at ACFE.com/fraudrisktools/tools.aspx.

[2] See Chapter 1 of the Guide for further information and guidance.

Checklist

- ☐ **Develop a comprehensive FRM policy.** There is not a one-size-fits-all FRM policy. The specific contents and language of your policy should be tailored to your organization's objectives, environment, and risk profile. The ACFE provides a sample fraud policy you can leverage as a foundation here.

- ☐ **Define roles and responsibilities for the FRM program.** The FRM roles and responsibilities of all personnel should be formally documented. This includes the board of directors, audit committee, senior management, business-enabling functions, risk and control personnel, legal and compliance personnel, and all other employees, as well as other parties interacting with your organization, such as contractors and customers.

- ☐ **Maintain and communicate a continuous focus on FRM.** This can be done in many ways, including:

  - » Implement an enterprise-wide mandatory fraud training. This type of training provides a consistent basis for fraud awareness throughout the organization, which is a fundamental pillar of any FRM effort.

  - » Embed periodic fraud awareness events to encourage discussion across all levels of your organization. For example, the ACFE hosts Fraud Week as a spearhead for building fraud awareness across the globe.

  - » Demonstrate FRM leadership. Executives should set an example by taking fraud matters seriously, adhering to controls and policies, and taking corrective action when others fail to do so.

- ☐ **Periodically assess the effectiveness of your organization's fraud awareness efforts and track progress or gaps over time.** This might include conducting an annual employee survey to assess how knowledgeable employees are about the FRM program covering topics such as: (1) employee knowledge of how to report ethical concerns or observed misconduct, (2) any observed misconduct (and whether such misconduct was reported), (3) the effectiveness of the organization's responses to verified or proven unethical behavior, and (4) employee ability to report unethical behavior or practice without the fear of retaliation.

- ☐ **Assess the effectiveness of the enterprise-wide mandatory fraud training** against the stated learning objectives using an established methodology, such as pre- and post-training surveys to compare the level of understanding of the skills and concepts before and after the seminar. Adjust the training approach and materials based on the results.

- ☐ **Adapt the enterprise-wide mandatory fraud training periodically** to address new fraud schemes, fraud risks, regulations, policies, etc.

FRAUD RISK ASSESSMENT

Play 3: Think Like a Fraudster

The Details

Identifying the likely fraud schemes that your organization is vulnerable to, 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. Figure 4 illustrates the concept of thinking like a fraudster. But where do you begin?

FIG. 4 Thinking Like a Fraudster

You can accomplish this effort by developing a comprehensive Fraud Risk Map, which identifies significant fraud scenarios across your entire organization. A Fraud Risk Map is a resource that outlines identified potential fraud schemes and other related information for each scheme, such as actor and fraud risk entry point, for various areas across your organization and is a resource you will be able to employ across your fraud risk management activities. For an example, see the sample **Fraud Risk Map**© template below.

FIG. 5 Sample Fraud Risk Map© Template

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.	• Any change to an employee's salary requires more than one level of approval
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.	• Payroll list is periodically reviewed for duplicate or missing Social Security Numbers (SSNs), home addresses or telephone numbers • Appropriate forms are completed and signed by the employee to authorize payroll deduction and withholding exemptions
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.	• Employees are required to submit detailed expense reports containing receipts, explanations, amounts, etc. • Supervisors are required to review and approve all reimbursement requests
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.	• Spending limits are in place to limit expenses on hotels, meals, etc. • Supervisors are required to review and approve all reimbursement requests

Utilizing the concept of *thinking like a fraudster*, you can work to identify and develop fraud scenarios based on known fraud events and investigations, existing risks identified through other risk management efforts, industry and general fraud risk research, and discussions with process owners and key stakeholders. The benefits of a fraud risk map are boundless; it will improve and provide your organization with a comprehensive understanding of fraud vulnerabilities and provide key inputs for the fraud risk assessment process. Further, the fraud risk map is an artifact that you can continue to refine and use to assess fraud risks going forward.

The following table outlines several of the Guide's points of focus related to the fraud risk assessment principle.[3] The points of focus detailed in this table *only* include those that apply to the identification of fraud risks. (For other points of focus related to fraud risk assessment, see Play 4.) You will also find key questions and a checklist, intended to help your organization develop a comprehensive fraud risk map, in line with the Guide's leading practices and guidance.[4]

Points of focus

- Includes entity, subsidiary, division, operating unit, and functional levels
- Analyzes internal and external factors
- Considers various types of fraud
- Specifically considers the risk of management override of controls
- Assesses personnel or departments involved and all aspects of the Fraud Triangle

Key questions

- How will you break down your fraud risk map to include your entire organization (i.e., subsidiaries, divisions, operating units, etc.)?
- What type of information do you want your fraud risk map to include? How can you translate that into an effective template?
- How might a fraud perpetrator exploit the any weaknesses in the system of controls?
  - » What internal fraud schemes is your organization vulnerable to?
  - » How could a perpetrator override or circumvent controls?
  - » Who might have a motive or incentive to commit fraud?
  - » What type of external fraud schemes is your organization vulnerable to?
- What types of fraud are most prevalent based on known fraud occurrences? What other internal data can you leverage to identify potential fraud schemes?
- Have you considered non-financial fraud risks and schemes?

[3] The ACFE developed Points of Focus Documentation Templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring. You can download these templates at ACFE.com/fraudrisktools/tools.aspx.

[4] See Chapter 2 of the Guide for further information and guidance.

Checklist

- ☐ **Determine how you want to break out your fraud risk map.** This can be by department, business function, etc. In line with guidance in the Guide, be sure to consider the entire enterprise and recognize that fraud can happen at any level or within any component of the organization. Further, ensure that the way you break out your fraud risk map aligns with how you plan to conduct your fraud risk assessment.

- ☐ **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. You can leverage Grant Thornton's Fraud Risk Map© Template and the ACFE's Risk Assessment and Follow-Up Action Templates to assist in developing a framework for your fraud risk map. While these resources can provide a useful starting point, you should tailor your fraud risk map to meet the needs and objectives of your FRM program and fraud risk assessment.

- ☐ **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. Key considerations include:

  - » **When identifying fraud schemes, do so in a group setting whenever possible.** Your efforts will benefit from conversations between relevant stakeholders who understand the functional area for which you are brainstorming fraud schemes.

  - » **Consider both the actor** (i.e., the perpetrator) and the **fraud risk entry points** (i.e., the function or process that 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.** For example, the ACFE's Fraud Tree outlines the complete classification of internal, or occupational, fraud, which you can use to identify any additional internal risks you might not have considered.

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

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

FRAUD RISK ASSESSMENT

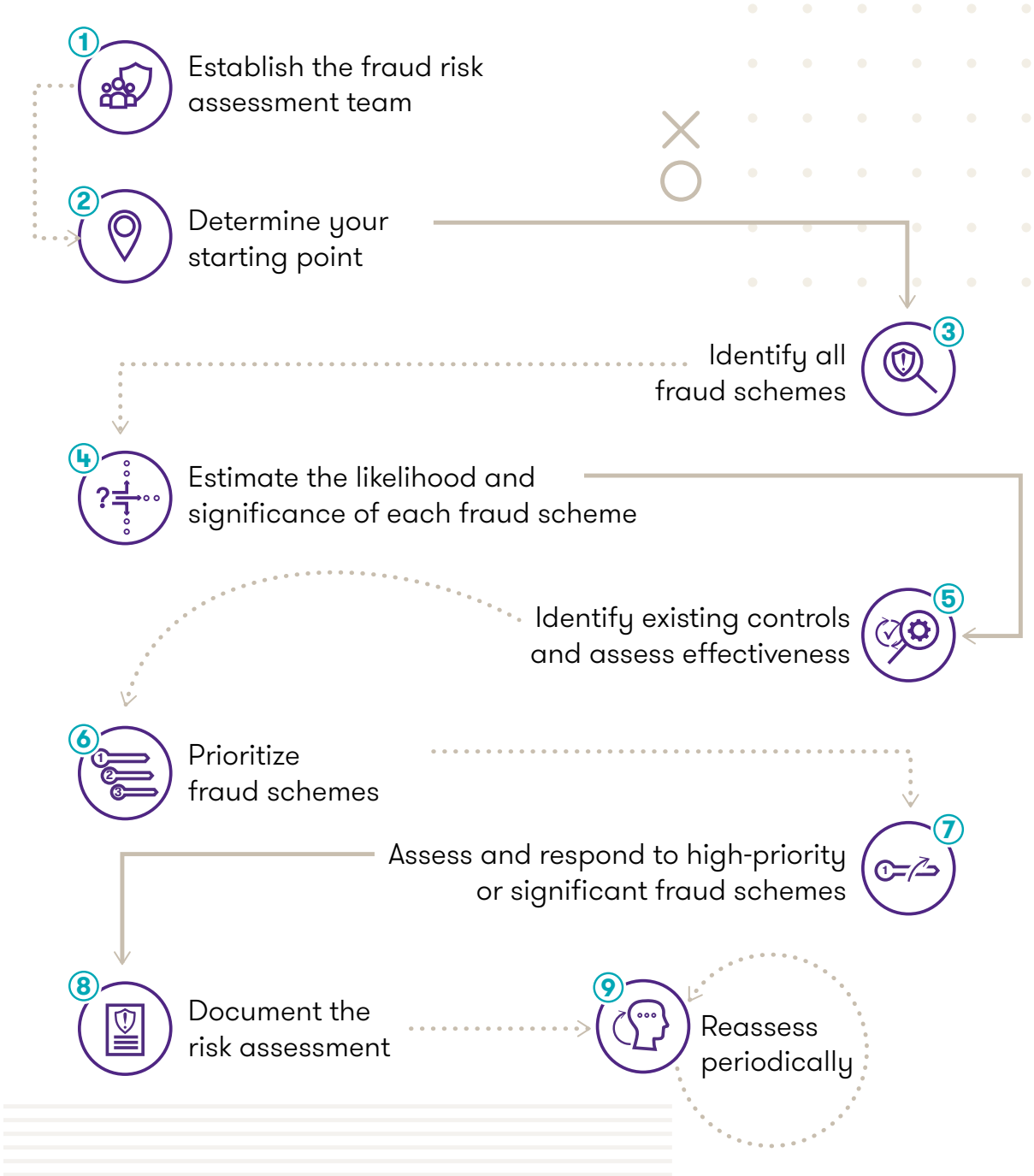
Play 4: Discover What You Don't Know

The Details

Conducting a fraud risk assessment helps you understand exactly where your processes might be vulnerable to fraud and allows for a holistic and detailed look at the fraud risks across the organization. Every enterprise faces a variety of risks from both internal and external sources, and a fraud risk assessment is a tool that your organization can leverage to identify and understand risks and provide the basis for how risks will be managed by your business. Further, the fraud risk assessment process is a proactive measure that can increase the perception of detection.

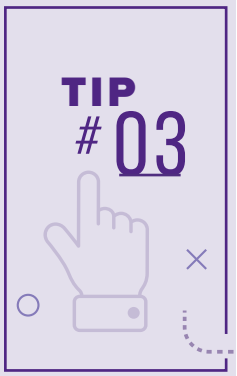
Therefore, the process should be visible throughout your organization, which means you should communicate broadly, promoting the process at all levels of the organization. It is important to remember that risk assessment is an art and not a science, so your fraud risk assessment methodology or approach should be tailored to the unique vulnerabilities and strategic goals of your organization. Generally, your assessment should include the steps shown in Figure 6.

FIG. 6 Steps of a Fraud Risk Assessment



The following table outlines several of the Guide's points of focus related to the fraud risk assessment principle.[5] The points of focus detailed in this table *do not* include those that apply to the identification of fraud risks. (For other points of focus related to fraud risk assessment, see Play 3.) You will also find key questions and a checklist, intended to help your organization conduct a comprehensive fraud risk assessment, in line with the Guide's leading practices and guidance.[6]

Points of focus	Key questions
• Involves appropriate levels of management • Estimates the likelihood and significance of risks identified • Identifies existing fraud control activities and assesses their effectiveness • Determines how to respond to risks • Uses data analytics techniques for fraud risk assessment and fraud risk responses • Performs periodic reassessments and assesses changes to fraud risk • Documents the risk assessment	• 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 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?



The ACFE has developed Risk Assessment and Follow-Up Action Templates that you can leverage throughout the fraud risk assessment process. This spreadsheet provides a risk assessment matrix for you to document your organization's fraud risks and controls. The template automatically creates a heat map showing the significance and likelihood of each identified fraud exposure, a fraud risk ranking page displaying each fraud risk exposure from most to least severe, and a control-activities matrix showing the identification and evaluation of existing control activities related to each fraud risk exposure. It also provides space to identify additional control activities and to record the organization's response plan for each exposure.

[5] The ACFE developed Points of Focus Documentation Templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring. You can download these templates at ACFE.com/fraudrisktools/tools.aspx.

[6] See Chapter 2 of the Guide for further information and guidance.

Checklist

- ☐ **Establish the fraud risk assessment team**, including clearly defining the members' roles and responsibilities and ensuring that the appropriate levels of management are involved. This should be informed by the established FRM governance structure and roles and responsibilities (see Play 2).

- ☐ **Determine your starting place.** You can either implement an enterprise-wide fraud risk assessment or a targeted fraud risk assessment. It might be beneficial to forgo an enterprise-wide assessment and instead conduct a pilot in a particular area to start small. This approach will allow you to test your methodology and implement lessons learned as you expand your assessment across other areas of the business. Either way, ensure that your starting place aligns to the roadmap and strategy you developed in Play 1.

- ☐ **Identify all fraud schemes.** (See Play 3.)

- ☐ **Estimate the likelihood and impact of each fraud scheme.** If your organization already has likelihood and impact scales developed for other risk management efforts, you might be able to leverage those here for consistency and to ensure that the fraud risk assessment results can roll up across your organization. You might also want to assess fraud risks on an inherent and residual basis. If you choose to do this, the key to this being effective is stakeholder communication to ensure understanding of these terms. Without that understanding, the results will not be insightful.

- ☐ **Identify existing fraud controls and their effectiveness.** Organizations usually have existing controls in place that serve as preventive or detective fraud control activities. As part of the fraud risk assessment process, the risk assessment team examines each specific fraud scheme or risk and identifies the existing related control activities. In some cases, there might be several existing controls. In other cases, the risk assessment team might conclude that no controls exist. After identifying existing control activities, the risk assessment team evaluates how effective these existing fraud control activities are in terms of mitigating fraud risk.

- ☐ **Prioritize fraud schemes.** Prioritizing risks will help you determine how to apply resources to effectively respond to the most important risks. In scoring and prioritizing risks, the risk assessment team should use the likelihood and impact assessments, as well as the presence and effectiveness of related control activities. For example, if a fraud risk lacks effective controls, it would be scored as a higher priority or a more significant risk than one with multiple effective controls in place.

- ☐ **Assess and respond to high priority or significant fraud schemes.** You may choose to strengthen existing control activities, add control activities, or consider using data analytics to combat high-priority or significant risks identified. Either way, the chosen response should align with your organization's fraud risk tolerance (see Chapter 2 of the Guide for details on developing your fraud risk tolerance) and the roadmap and strategy you developed in Play 1.

- ☐ **Document the risk assessment.** This can be done in a number of ways, but key items to document include the methodology deployed, the assessment results, and the organization's response strategies.

- ☐ **Reassess periodically**, considering changes external to the organization, operational changes, and leadership changes.

As part of the fraud risk assessment process, you should conduct qualitative assessment techniques, such as:

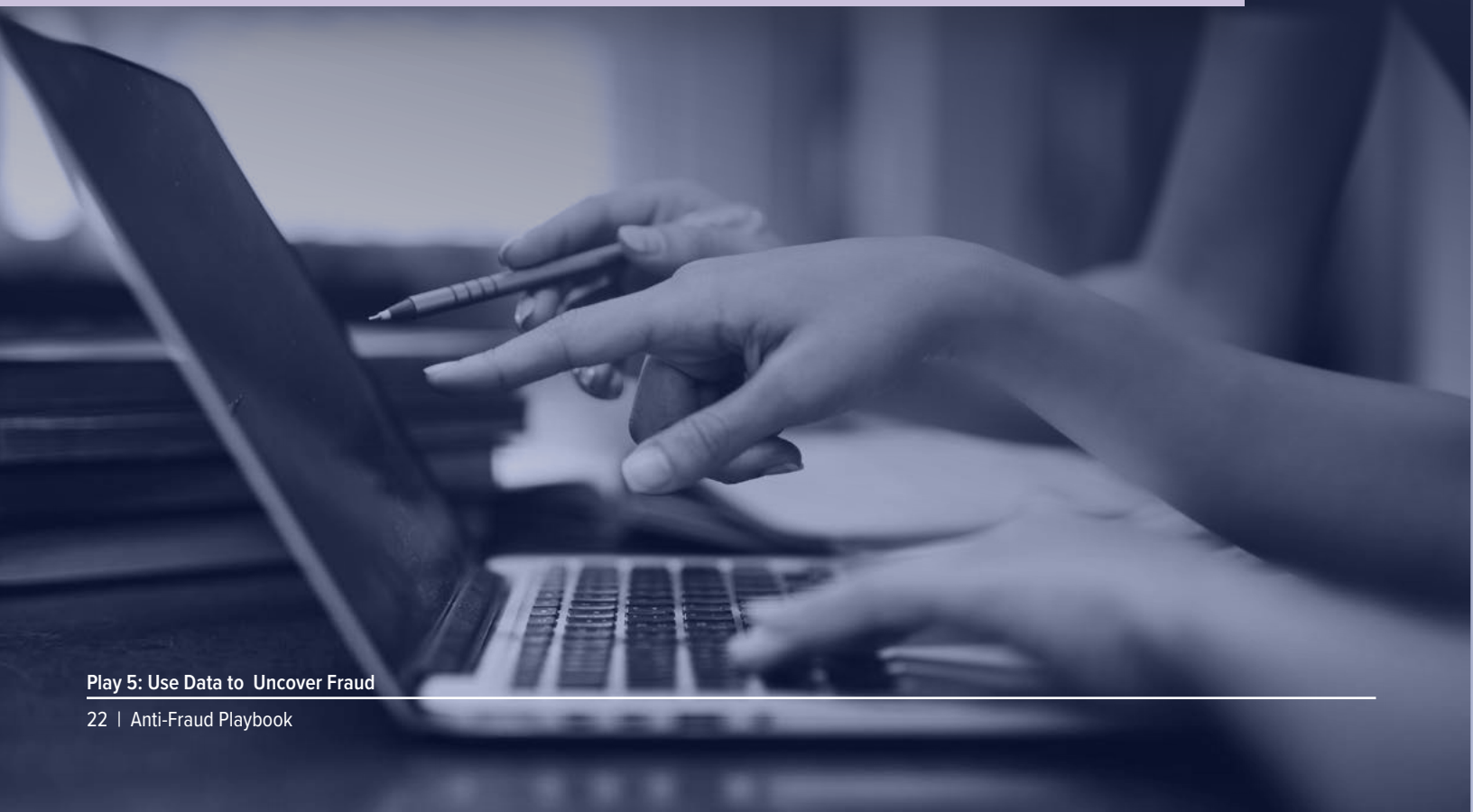
- Interview relevant stakeholders who understand the functional area for which you are assessing risk. These conversations should include an open discussion on fraud risk, the identification of relevant controls, and efforts to get to a consensus on risk scoring.
- Conduct cross-functional risk workshops, which are considered the gold standard of qualitative risk assessment techniques. Benefits of these sessions include the ability to consider fraud risk interactions across operations, break down silos across business areas, and facilitate meaningful discussions about how various processes and risks interrelate.

FRAUD CONTROL ACTIVITIES

Play 5: Use Data to Uncover Fraud

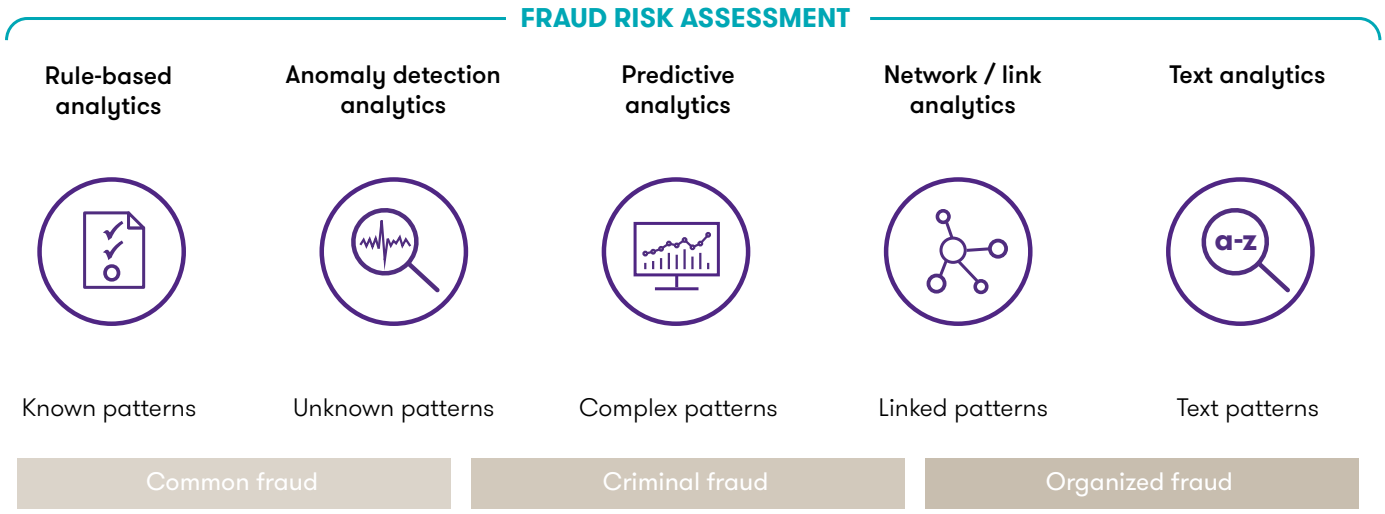
The Details

The use of data analytics is a powerful fraud prevention, detection, and investigation tool, making it an important part of an effective and holistic FRM program. Many anti-fraud analytics tests can be easily implemented using basic spreadsheet software, while the most advanced organizations are leveraging robotics, machine learning, and artificial intelligence to enhance their anti-fraud analytics programs. Whether basic or complex, data analysis of some sort is critical for elevating your organization's fraud detection and prevention efforts. When in doubt, start small with a pilot approach to reduce initial investment and gain quick wins for your organization's FRM program.



There are a lot of analytic techniques out there, and each one brings with it unique benefits and insights. However, not all analytic techniques are equal—certain techniques are better suited for certain objectives or analyses than others. Figure 7 outlines five different analytic techniques ranging from simple to more advanced. This is not a comprehensive listing; there are many options out there and what you choose depends on your organization's priorities.

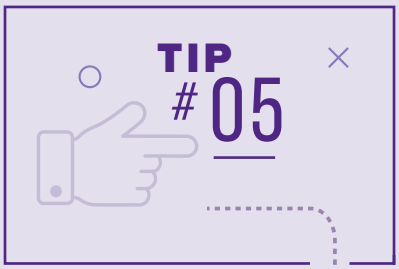
FIG. 7 Example Analytic Techniques



When implementing your anti-fraud analytics program, it's important to note two things: First, you can and should leverage the results of your fraud risk assessment (see Play 4) to inform your analytics strategy and priorities. Second, your analytics capabilities will evolve with your FRM program. For example, over time you should consider integrating advanced analytics procedures, such as text mining, statistical analysis, and pattern/link analysis, to further your capabilities and enhance your anti-fraud analytics program. As a robust anti-fraud analytics effort is established in your organization, you may choose to combine the techniques above or to integrate them via a software platform. Doing so will take your organization from a reactive approach to a predictive approach, enabling you to identify instances of potential fraud before they even occur.

The following table outlines one of the Guide's key points of focus related to the fraud control activities principle.[7] This table only includes the point of focus that applies to data analytics. You will also find key questions and a checklist, intended to help your organization implement data analytics to combat fraud, in line with the Guide's leading practices and guidance.[8]

Points of focus	Key questions
• Uses proactive data analytics procedures	• Who will be responsible for your anti-fraud analytics program? • How can your FRM strategy (see Play 1) help you decide what priority level of fraud schemes (see Play 4) you will target with analytics? • What data is available related to your selected fraud schemes? Who are the relevant stakeholders you will need to work with to access and collect this data? Will you need to integrate data from multiple sources? • What analytics techniques and tests will you implement? What resources and level of investment will be required? • What type of reporting will be required? What stakeholders will you report results to, and how often will reporting occur? • How will findings be remediated and corrected? How will you integrate this process with the fraud risk assessment (see Play 4)?



The ACFE developed an Anti-Fraud Data Analytics Tests interactive tool, which provides numerous data analytics tests that can be used to help identify the red flags of various occupational fraud schemes. This tool is based on the structure of the ACFE's Fraud Tree. You can drill down to a specific scheme type and see data analytics tests that are relevant to that fraud risk.

[7] The ACFE developed Points of Focus Documentation Templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring. You can download these templates at ACFE.com/fraudrisktools/tools.aspx.

[8] See Chapter 3 of the Guide for further information and guidance.

Checklist

The following checklist provides a framework for implementing an anti-fraud analytics program. It is important to take an iterative approach to analytics, so you can ensure that tests are designed and validated carefully. Further, the implementation of analytics should align with your overall FRM roadmap and strategy (see Play 1). You will also need to determine who will be responsible for your anti-fraud analytics program, which should be informed by the established FRM governance structure and roles and responsibilities (see Play 2).

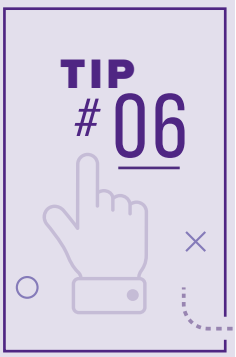
- ☐ **Design your analytics.** Map the prioritized fraud schemes identified through your fraud risk assessment (see Play 4) to potential data sources and assess availability of relevant data. Once data is identified and availability is confirmed, determine the analytic techniques and tests you wish to implement.

- ☐ **Collect the data.** Work with relevant stakeholders across your organization to collect data. As part of this process, you will need to extract, transform/normalize, and validate the data to ensure that it will provide meaningful results when analyzed (i.e., to avoid "garbage in, garbage out").

- ☐ **Execute your analytics techniques and tests.** As execution proceeds, iterate and modify based on the data received, data quality, user feedback, and test results. This process will be ongoing and will require refining your models as needed to ensure the effectiveness of the techniques and the accuracy and relevance of the results.

- ☐ **Report your findings and observations to relevant stakeholders.** Reporting should be in line with the established FRM governance structure (see Play 2). For example, if a potential fraud event is uncovered, then it should be referred to your organization's investigative body as outlined in your fraud risk policy. However, reporting should not stop there. You should report on key outcomes to other relevant stakeholders to ensure your findings and observations inform the FRM program and lead to lessons-learned that can be incorporated to strengthen current controls and mitigating activities. For example, if your intended audience is senior leadership, then presenting your findings and recommendations in a visual manner and focusing on the most important items needed for decision-making may be best. However, if you are presenting to business unit stakeholders, then tailor the results to highlight the items that affect their day-to-day work or items that they have ownership of so that they are aware of their risks and can begin work on mitigating them.

- ☐ **Implement remediation and corrective actions activities** based on the response strategies identified through your fraud risk assessment (see Play 4) and the established FRM governance structure (see Play 2). For example, if your results indicate that one type of fraud is a significant concern, then that information should feed back into your fraud risk assessment results to inform the response strategy and risk prioritization. Remember, all remediation and corrective action should also align to your overall FRM strategy and your long-term goals and vision of your FRM program (see Play 1).



Data analytics is only one type of control activity that your organization should consider. You should design and implement a multitude of controls to prevent and detect fraud, and the range of control activities varies from one organization to the next. If you are unsure of what types of control activities you need to implement, the results of your fraud risk assessment (see Play 4) can inform what areas you should prioritize and the types of controls you need to implement to combat high-priority risks.

FRAUD CONTROL ACTIVITIES

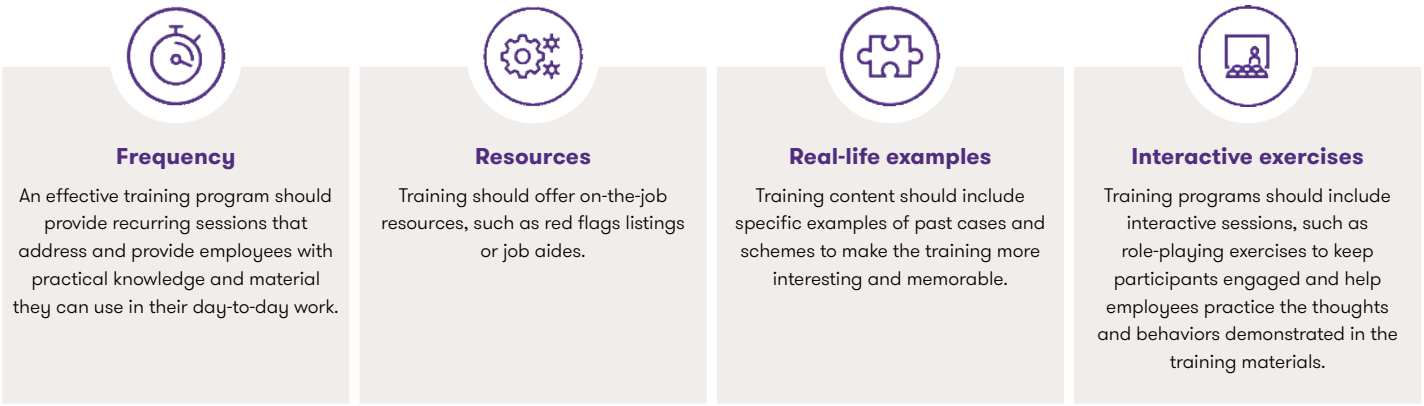
Play 6: Knowledge Is Power

The Details

Play 2 covered the need to develop and deploy mandatory enterprise-wide anti-fraud training. However, training shouldn't stop there. Customizing the content and delivery of the training based on the specific roles of different employees (or teams of employees) results in employees better connecting the message of the training to their day-to-day responsibilities. 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. Further, through the training, management can communicate its commitment to high ethical standards and fraud prevention.

As you develop your targeted and role-based anti-fraud training program, consider the best practices shown in Figure 8:

FIG. 8 Training Best Practices



The following table outlines the key questions and a checklist, intended to help your organization conduct a maturity assessment and develop a targeted and role-based anti-fraud training program, in line with the Guide's leading practices and guidance.

Key questions

- What resources are available to help design your targeted and role-based anti-fraud training program? Who will be responsible for the anti-fraud training program?
- What information is available to help you determine your training needs, such as a fraud risk assessment (see Play 4) or internal audit findings?
  - » Where is your organization particularly vulnerable to fraud based on your fraud risk assessment? (See Play 4.) Which departments or groups within your organization have the lowest level of fraud awareness? (See Play 2.)
- What fraud-related trainings do you already have in place? How can these be expanded upon?
- How can you assess the effectiveness of your anti-fraud training? How will updates or revisions be made to the training content and delivery?

Checklist

☐ **Determine who is responsible for the development and oversight of the targeted role-based training program.** This should align to the established FRM governance structure (see Play 2) and should define roles and responsibilities across the monitoring process.

☐ **Determine where to focus your training efforts** based on the results of other FRM activities. For example, you might choose to focus on an area of the business with the highest level of fraud risk or the most significant control gaps as determined by your fraud risk assessment.

☐ **Develop your training materials.** Consider the training best practices noted in Figure 8. If you already have training content, determine how this can be enhanced or expanded upon for the area you are focusing on.

☐ **Deliver your targeted role-based training.**

☐ **Evaluate the effectiveness of the training and adapt it periodically.** Following delivery, evaluate the effectiveness of your training using an established methodology and adapt the training periodically based on both the results of your evaluation and on any changes in organization's fraud risks or operations. You can leverage the processes you have in place for enterprise-wide anti-fraud training (see Play 2) to perform these steps for your targeted role-based training efforts as well.

FRAUD INVESTIGATION AND CORRECTIVE ACTION

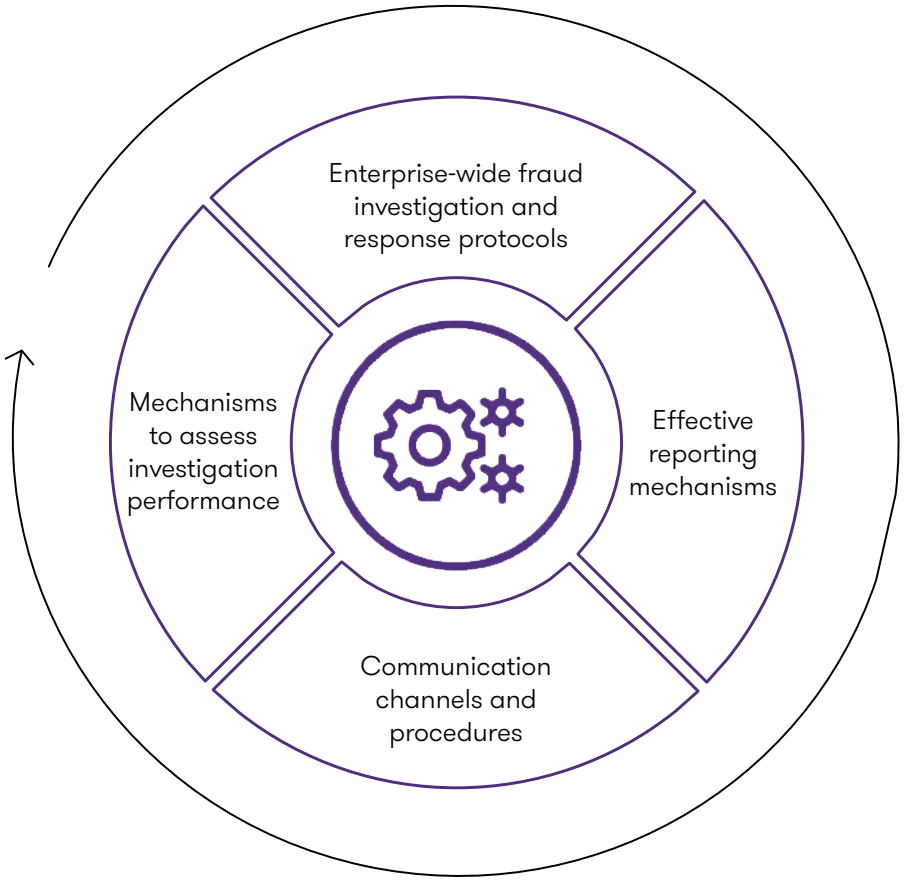
Play 7: Lay the Groundwork for Investigations

The Details

You've received allegations of fraud. What's next? Mechanisms to conduct thorough forensic investigations to understand the root causes of fraud and undertake corrective actions to address those root causes are essential components of a holistic and effective FRM program.

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 fraud risks to mitigate fraud effectively. Figure 9 illustrates the key elements necessary to lay the groundwork for investigations and encourage tips.

FIG. 9 Key Elements to Lay the Groundwork for Investigations



The following table outlines several of the Guide's key points of focus related to the fraud investigation and corrective action principle.[9] The points of focus detailed in this table *only* include those that apply to laying the groundwork for fraud investigations. (For other points of focus related to fraud investigation and corrective action, see Play 8.) You will also find key questions and a checklist intended to help your organization implement effective investigation and response protocols in line with the Guide's leading practices and guidance.[10]

Points of focus	Key questions
• Establishes fraud investigation and response protocols, including: » Mechanisms to communicate investigation results » A corrective action process » Mechanisms for evaluating investigation performance	• Does your organization have established enterprise-wide fraud investigation and response protocols? Is there a formal process for receiving, evaluating, and responding to reports of potential fraud? • Who will be responsible for conducting fraud investigations? Does your organization have sufficient in-house resources to conduct these investigations? • What system does your organization have for receiving allegations of potential fraud? Are there documented protocols for proper use and monitoring of this system? • Does your organization have a whistleblower protection program, such as a no-retaliation policy, in place? • Does your organization have established communication mechanisms to report investigation results both internally and externally? • Does your organization have established processes for utilizing investigation results to improve processes or close potential control gaps? • Does your organization have mechanisms in place to periodically assess the effectiveness of investigations and solicit objective feedback on the process?

[9] The ACFE developed Points of Focus Documentation Templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring. You can download these templates at ACFE.com/fraudrisktools/tools.aspx.

[10] See Chapter 4 of the Guide for further information and guidance.

Checklist

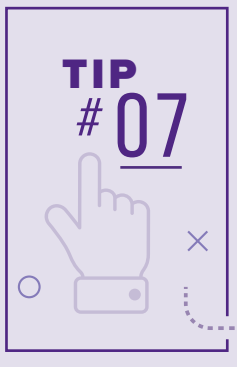
- ☐ **Establish enterprise-wide fraud investigation and response protocols.** These protocols should align with the established FRM governance structure (see Play 2), as they are important inputs to your organization's overall fraud response plan. In addition, these protocols should define roles and responsibilities across the investigative process, including who is responsible for conducting investigations.

- ☐ **Assess your organization's current reporting mechanisms.** Promoting and supporting open communication and tips is vital to ensuring the effectiveness of reporting mechanisms and is a key element of an effective anti-fraud culture (see Play 2). You should assess current mechanisms to determine if they are adequately marketed and effectively operating, as well as whether any additional mechanisms should be added. For example, ensuring that you market reporting mechanisms to both internal and external parties and ensuring that you have an established whistleblower protection program in place will enhance the effectiveness of your reporting mechanisms.

- ☐ **Establish communication channels and procedures.** Following the conclusion of an investigation, you should have a clear path for disseminating the results of investigations, as necessary, in line with your established FRM governance structure (see Play 2). Communication procedures should cover items such as closing the feedback loop with the reporting party (as applicable) and reporting lessons learned to relevant stakeholders to improve controls and processes in place.

- ☐ **Establish monitoring mechanisms to ensure implementation of corrective action following a fraud investigation.** Communicating the results is the first step. Ensuring that there are monitoring mechanisms in place to track progress on corrective actions following an investigation is key to closing identified control gaps.

- ☐ **Establish mechanisms to assess investigation performance.** Solicit objective feedback on the effectiveness of your investigations process, such as a formal procedure for initiating an anonymous survey.



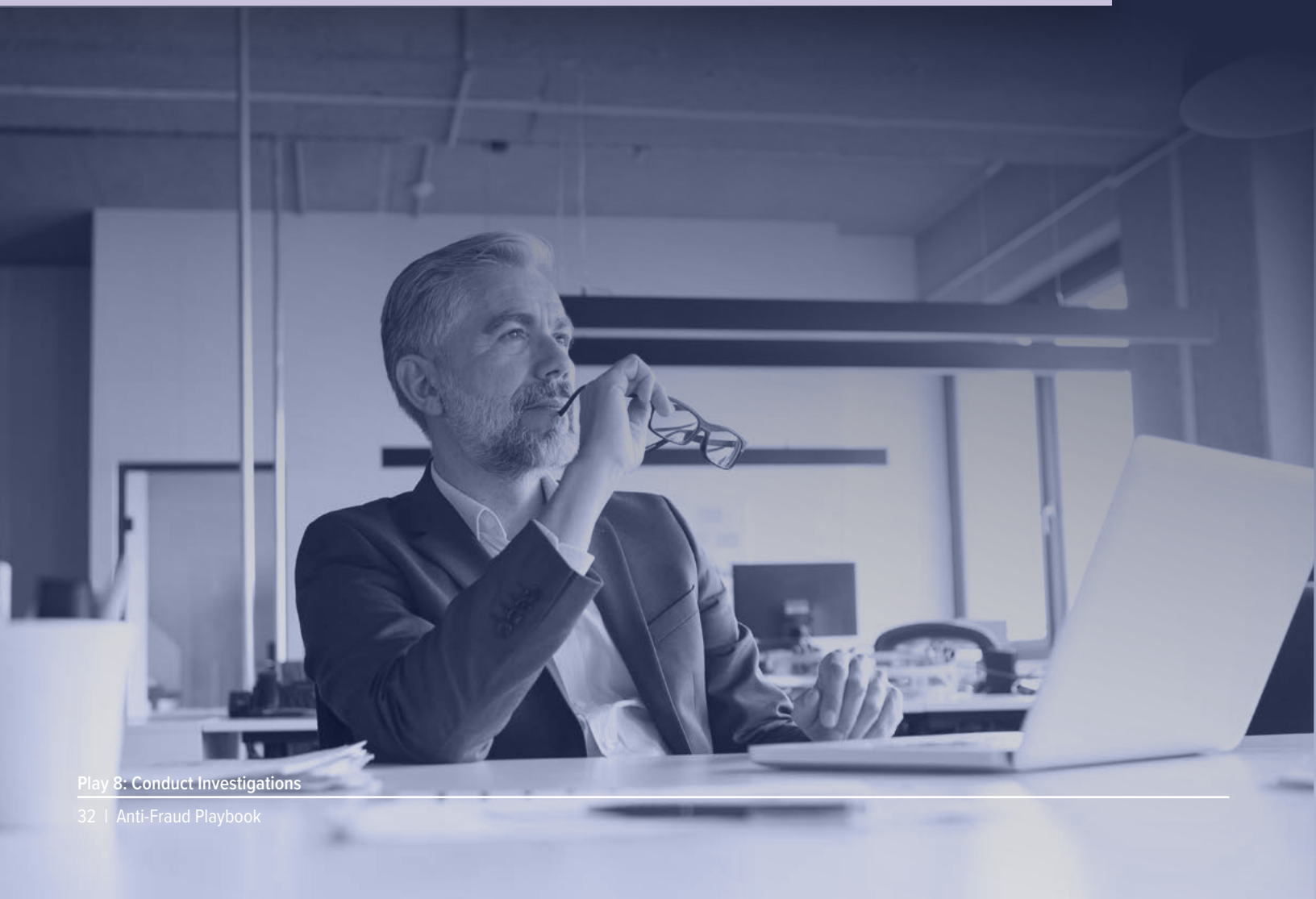
It is a best practice implement a central repository for allegations and complaints, such as a case management system. The ACFE's Risk Assessment and Follow-Up Action Templates provides a spreadsheet that your organization can leverage to track cases and monitoring efforts in a single place.

FRAUD INVESTIGATION AND CORRECTIVE ACTION

Play 8: Conduct Investigations

The Details

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.



Because they are a critical component of the FRM program, all investigations should be conducted with integrity and objectivity. Figure 10 details the typical components and factors to consider as part of conducting investigations.

FIG. 10 Typical Components and Factors to Consider for Investigations

Investigations will typically include the following components:	The investigation will involve different steps depending on the kind of allegation, but below are some general factors to consider:
Evidence gathering	Time sensitivity
Computer forensics	Confidentiality
Develop and test hypotheses	Legal privileges
Gather external records	Objectivity
Witness interviewing	
Perform data analysis	

The following table outlines several of the Guide's key points of focus related to the fraud investigation and corrective action principle.[11] The points of focus detailed in this table only include those that apply to conducting investigations. (For other points of focus related to fraud investigation and corrective action, see Play 7.) You will also find key questions and a checklist, intended to help your organization conduct effective fraud investigations in line with the Guide's leading practices and guidance.[12]

Points of focus	Key questions
• Conducting investigations, including: » Communicating investigation results » Taking corrective action » Evaluating investigation performance	The following key questions focus on the elements and considerations in developing an effective investigative work plan: • Do you have a documented investigative work plan to guide each investigation? • How will you ensure that investigations are conducted independently without influence? • How might the work plan change from investigation to investigation? • How might the work plan expand or contract based on facts discovered during the investigation? • How does your organization assess the scope, severity, credibility, and implications of potential fraud? Is this clear in the work plan? • How does your organization determine discipline, remediation, asset recovery, or other activities to address the findings of an investigation? Is this clear in the work plan? • Does the investigation team have access to subject-matter experts if needed, including forensic accountants and experts in fields such as computer forensics? • What actions are taken upon the completion of an investigation, such as disciplinary action, training, and civil action? How is the appropriate action determined?

[11] The ACFE developed Points of Focus Documentation Templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring. You can download these templates at ACFE.com/fraudrisktools/tools.aspx.

[12] See Chapter 4 of the Guide for further information and guidance.

Checklist

The following checklist outlines high-level steps needed to conduct an investigation. However, this process should align with and be guided by your established investigation and response protocols (see Play 7). Planning is essential to an effective investigation; as such, the foundation of your investigation is rooted in your investigative work plan.

- ☐ **Develop the investigation work plan.** Your investigative work plan should define and assign each investigative task to the appropriate team member. The plan should prioritize tasks and should be iterative as the investigation is carried out based on facts uncovered.

- ☐ **Implement the investigative work plan.** As the work plan is implemented, consider changes based on the unique circumstances of the investigation. During this stage, the investigative team will gather evidence, perform analysis, conduct interviews, etc. The team will need to document and track information related to steps taken and information collected.

  - » If allegations are substantiated or appear as if they are likely to have occurred, the investigative team will need to evaluate the root cause.

Following the investigation, several steps should be implemented to close the loop, as defined in Play 7:

- ☐ **Communicate the results,** leveraging established communication channels and procedures.

- ☐ **Take corrective actions and monitor implementation,** leveraging established monitoring mechanisms to ensure effective implementation of corrective action following a fraud investigation.

- ☐ **Evaluate investigation performance,** leveraging established mechanisms for performance evaluation to solicit objective feedback.

FRAUD RISK MANAGEMENT MONITORING ACTIVITIES

Play 9: Monitor Your Progress

The Details

Ongoing monitoring and periodic evaluations provide vital insight into the effectiveness of FRM activities and help identify areas for improvement. Monitoring and periodic evaluations should cover the full spectrum of your FRM program, and at a high level include two key steps: (1) implementing monitoring and evaluation activities and (2) using the results to improve your FRM program. These are highlighted in Figure 11.

FIG. 11 **Monitoring Activities Overview**

Monitor and evaluate the effectiveness of FRM activities

- To be effective, this process should focus on measuring the outcomes of those activities instead of simply reviewing the outputs. For example, instead of focusing on the number of attendees who completed anti-fraud training (the output), you can focus on the results of the evaluations to determine how fraud awareness and understanding has improved over time.
- Examples of activities to monitor include fraud risk assessments (see Play 4), enterprise-wide anti-fraud training (see Play 2), targeted anti-fraud trainings (see Play 6), and your analytics activities (see Play 5).

Use the results to improve FRM activities

- You should then use the results of monitoring and evaluations to improve FRM activities at your organization.
- For example, let's say you were evaluating the effectiveness of a targeted role-based anti-fraud training (see Play 6) using a survey, and the results were lower than expected. This would indicate that the outcome of the training was not adequately achieved and that the training should be improved to achieve the desired outcome.

The following chart outlines the Guide's key points of focus related to the fraud risk management monitoring activities principle.[13] You will also find key questions and a checklist, intended to help your organization implement effective monitoring and evaluation activities, in line with the Guide's leading practices and guidance.[14]

Points of focus

- Considers a mix of ongoing and separate evaluations
- Considers factors for setting the scope and frequency of evaluations
- Establishes appropriate measurement criteria
- Considers known fraud schemes and new fraud cases
- Evaluates, communicates, and remediates deficiencies

Key questions

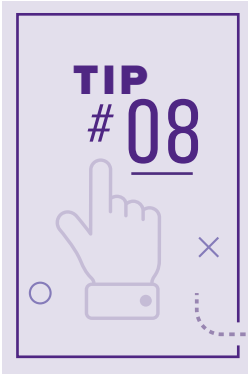
- Who will be responsible for the FRM monitoring program?
- What ongoing monitoring evaluations are key to assessing the performance and effectiveness of your FRM program?
- What separate evaluations, such as internal audit or external reviews, are key to assessing the performance and effectiveness of your FRM program?
- How frequently should FRM monitoring activities be performed?
- What factors may affect the scope of FRM monitoring activities? How may these changes affect scope or frequency of evaluations?
- What measurement criteria will be used to evaluate the FRM program?
- How will the results of FRM monitoring activities be communicated across the organization and to relevant stakeholders?
- How will deficiencies identified by FRM monitoring activities be remediated?

[13] The ACFE developed Points of Focus Documentation Templates to help create consistent and uniform documentation related to fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring. You can download these templates at ACFE.com/fraudrisktools/tools.aspx.

[14] See Chapter 5 of the Guide for further information and guidance.

Checklist

- ☐ **Determine who is responsible for oversight of the monitoring and evaluation efforts.** This should align with the established FRM governance structure (see Play 2) and should define roles and responsibilities across the FRM monitoring process.
- ☐ **Determine the type of monitoring and evaluation activities you plan to implement,** ensuring that all components of your FRM program are covered. For example, you should:
  - » **Conduct periodic evaluations and reassessments** of the FRM program, including reassessing for each of the five principles outlined in the Guide. For this type of reassessment, you can leverage Grant Thornton's Enterprise Anti-fraud Maturity Assessment Model© and the ACFE's FRM Scorecards.
  - » **Implement ongoing evaluations for fraud control activities and fraud risk mitigation activities,** as identified and implemented as part of your fraud risk assessment (see Play 4). For example, you can leverage data analysis to identify exceptions or deviations from key processes related to control activities to determine if the control is operating properly.
- ☐ **Set the scope and frequency of monitoring and evaluation activities.** For example, if you plan to conduct targeted evaluations of your anti-fraud training initiatives, you may decide that this should occur ad hoc (frequency) and be focused specifically on each occurrence of a new training program or topic (scope).
- ☐ **Establish measurement criteria for selected monitoring and evaluation activities.** For example, your measurement criteria for investigative performance might be based on the evaluation results.
- ☐ **Perform both ongoing and separate monitoring and evaluation activities.**
- ☐ **Implement corrective actions based on the results of monitoring activities,** as needed. 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 and evaluations are proactive measures that can increase the perception of detection. Therefore, similar to the fraud risk assessment process (see Play 4), the monitoring and evaluation processes should be visible and communicated throughout your organization.

FRAUD RISK MANAGEMENT MONITORING ACTIVITIES

Play 10: Report on Your Progress

The Details

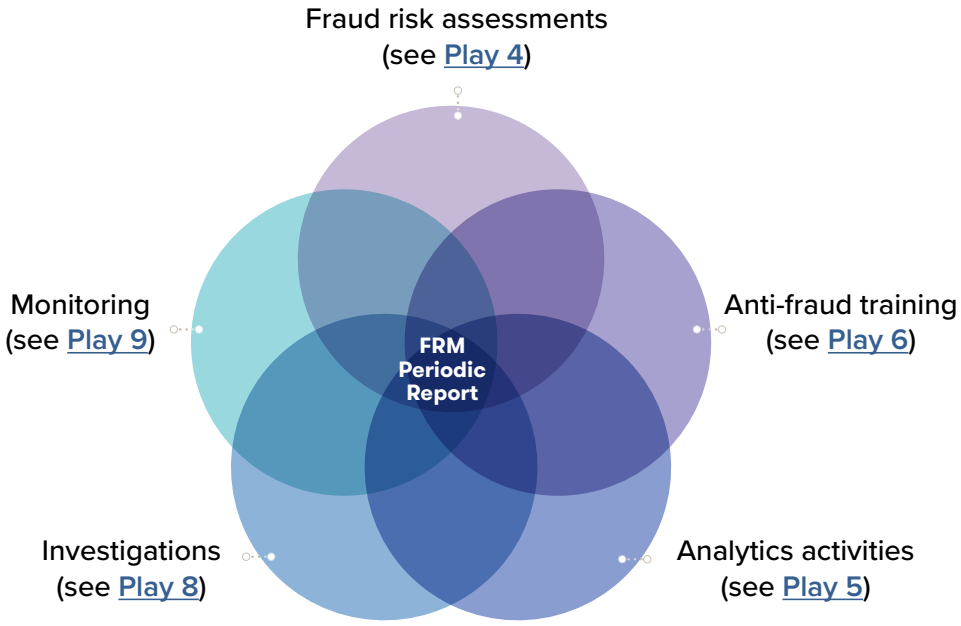
Communicating the results and outcomes of your FRM program at all levels of your organization—and to your organization's leadership—is essential to increase awareness of the FRM program, showcase the program's accomplishments, and motivate senior leaders to prioritize FRM efforts. This concept should not be new; the importance of making your anti-fraud efforts visible and communicated across the organization has been emphasized throughout this playbook. However, that is just one piece of the puzzle.

Communicating along the way is important, but ensuring that you communicate results, insights, and takeaways on a periodic basis to relevant parties at all levels of your organization will take your FRM activities to the next level. The bottom line is that you can and should tell the story of your FRM efforts in aggregate; without doing so, you miss an opportunity to not only showcase the value of your efforts, but also to improve anti-fraud efforts overall.

The information that should be shared with leadership or across the organization can vary depending on the nature of the information. Figure 12 outlines various considerations as you develop your periodic FRM report.

As part of your report development, ensure that you consider these factors both individually and together. You might be surprised to see new insights when you look at the information as a whole rather than only looking at the factors individually.

FIG. 12 Developing Your FRM Report



The following table outlines the key questions and a checklist, intended to help your organization in developing an FRM reporting approach, in line with the Guide's leading practices and guidance.

Points of focus

- Who are your target audiences for periodic reporting?
- How frequent should you distribute a periodic FRM report? Does this differ for different audiences?
- What insights have you gathered from your FRM activities, considering activities both separately and in aggregate?
- What key accomplishments have been made related to your FRM activities?
- What delivery method or methods will be used for reporting? How does this differ for different audiences?

Checklist

- ☐ **Determine target audiences.** You may develop different reports for your board of directors or senior leadership than you would for individual business units or functions. So, understanding who you plan to target will be key to developing the right messages.
- ☐ **Determine the frequency of reporting.** This may differ for different audiences. For example, you may report annually to senior leadership and quarterly to leadership within the FRM program.
- ☐ **Identify the key insights and accomplishments.** Consider key insights and accomplishments both across individual activities and at an aggregate level to identify trends, patterns, and other relevant data points to showcase the program's accomplishments and changes. Similar to monitoring, it is best to focus on measuring the outcomes of FRM activities rather than simply reviewing outputs.
- ☐ **Deliver your report** in line with established frequency of reporting.
- ☐ **Evaluate the effectiveness and impact of reporting** and make changes based on the results and feedback.
- ☐ **Iterate** based on established frequency of reporting.

In determining how best to communicate insights and outcomes and to showcase program accomplishments to leadership and across the enterprise, make sure to consider your organizational structure, corporate culture, and the intended audience. You may want to consider the use of reports, dashboards, or other visual representations of relevant information based on what has been shown to work in reporting on similar initiatives in your organization.

The ACFE/COSO Fraud Risk Management Guide outlines five key principles: fraud risk governance, fraud risk assessment, fraud control activities, fraud investigation and corrective action, and fraud risk management monitoring activities. While frameworks like this are a useful reference, they are most beneficial when put into practice. This playbook provides readers with practical advice and guidance on how to implement those key principles.

The fraud risk journey looks different for every company. One size does not fit all. As the first Play suggests, fraud risk management should be customized to meet the unique needs of each organization. A good fraud risk management program has relevance and context, in order to match the culture and broader objectives of the corporation.

As Plays 9 and 10 reinforce, fraud risk management is not a set-and-forget exercise. The economic and regulatory environments in which companies operate are subject to change. Leading organizations should plan continuous improvement to their fraud risk program as they face a constantly evolving fraud risk landscape.

Use this Playbook as the foundation to develop a custom fraud risk management approach for your company and move from theory into practice.

Appendix

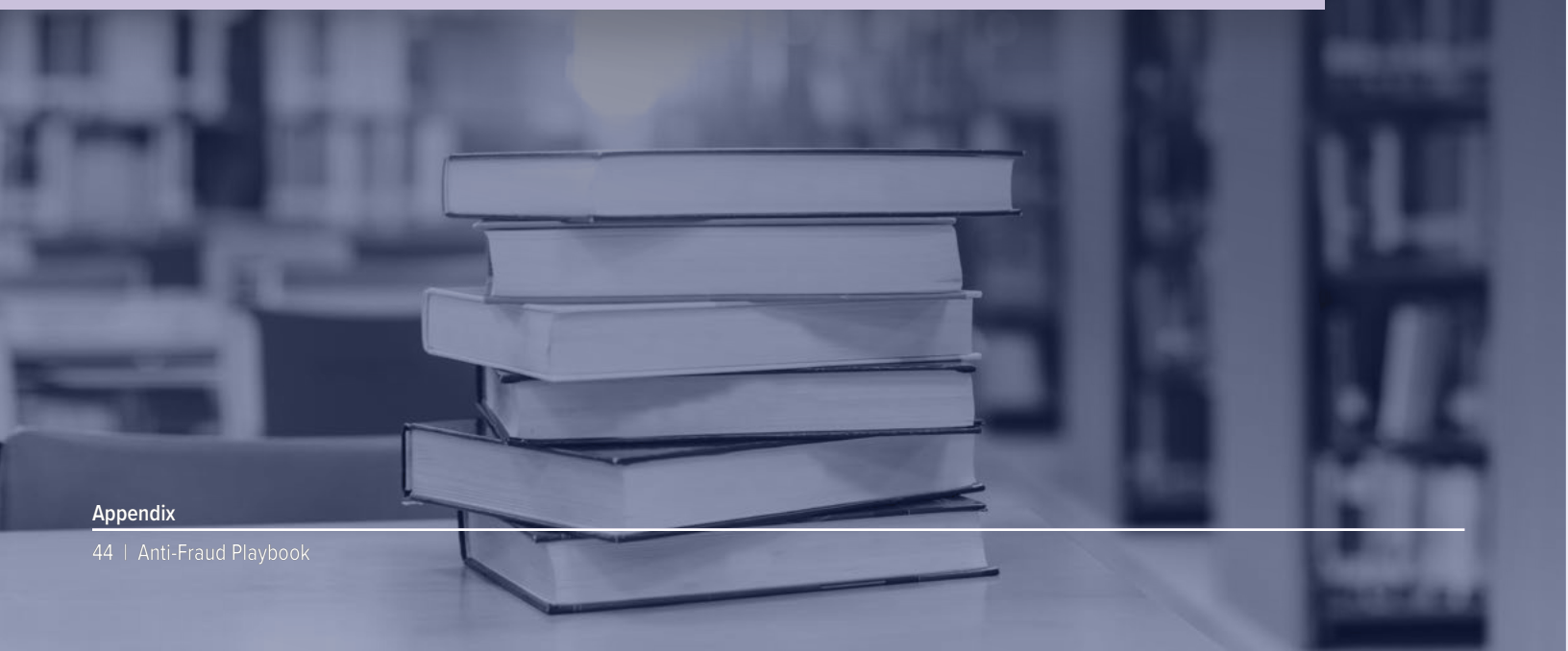
Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

by COSO Category

1. Fraud Risk Governance
2. Fraud Risk Assessment
3. Fraud Control Activities
4. Fraud Investigation and Corrective Action
5. Fraud Risk Management Monitoring Activities

Appendix B: Fraud Risk Map Template

Appendix C: Implementation Checklists



Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

COSO Category	1 - AD HOC	2 - INITIAL
Fraud Risk Governance 	Organization does not have a documented Fraud Risk Management Policy. Organization has not made commitment to Fraud Risk Management, and fraud awareness is not emphasized from the top down. Organization does not have a formalized Fraud Risk Management Program. Roles and responsibilities are not communicated to all levels of the organization. Fraud awareness training does not come from a consistent source or on a scheduled timeline.	Organization has a Fraud Risk Management Policy, but it is not reviewed and understood across all levels of the organization. Organization is aware of the need for a formal Fraud Risk Management Program, but has not received full "buy-in" from employees across all levels of the organization. The program has not been completely implemented in all business units. A Fraud Risk Management Program is in place, but fraud risk management roles and responsibilities are not consistently understood throughout the organization. There is a siloed approach to managing fraud risks. Fraud awareness training materials are developed, but its importance is not stressed and completion is not formally tracked.
Fraud Risk Assessment 	Organization has not established a Fraud Risk Assessment Team with appropriate levels of management considering all organizational components. A Fraud Risk Assessments are not periodically performed by the organization. The Fraud Risk Assessment methodology, process, and results are not documented.	Organization has a team of individuals that perform risk assessments across the organization, for example within the Internal Audit function. Risk assessments are performed across different facets of the organization, but the focus is not specific to "fraud risk." Fraud risk may be considered in these risk assessments. Risk assessment methodology, process, and results are documented.

Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

Strength Level

3 - REPEATABLE	4 - MANAGED	5 - LEADERSHIP
Organization has a documented Fraud Risk Management Policy that is reviewed and periodically updated by management. Organization has established commitment to Fraud Risk Management through their tone at the top. Employees of the organization understand the commitment to Fraud Risk Management, but it is not a priority. The Fraud Risk Management Program is documented and place with clearly identified roles and responsibilities. Fraud awareness training is formally scheduled and tracked.	Organization has a formally documented Fraud Risk Management Policy that is periodically reviewed and updated by management. Periodic review should consider whether changes to organizational structures and methods are needed. Fraud risk management activities cut across all processes, business lines and geographies. Organization has made a firm commitment to Fraud Risk Management and has established a strong tone at the top and may include a Fraud Risk Management Team who reports to C-level management. Periodic fraud awareness training incorporates known fraud schemes in the industry and from past experiences. Organization has a formalized and documented Fraud Risk Management Program and the organization understands how ERM and fraud risk management are interrelated and can leverage knowledge and capabilities.	A dedicated Fraud Risk Management Team has clearly defined roles and responsibilities responsible for Fraud Risk Management Program oversight and continuous improvement. Management frequently communicates a strong tone at the top stressing the organization's commitment to Fraud Risk Management. Organization has a formalized and documented Fraud Risk Management Program and has disseminated the importance of fraud awareness through frequent communication to all levels of the organization. Emerging risks learned from external and internal sources are incorporated into scheduled fraud awareness training that is tracked. As fraud risks evolve, the awareness training, processes, and controls are quickly reacted to.
Organization has a team of individuals within management that perform enterprise-wide fraud risk assessments on a scheduled basis. Fraud Risk Assessment methodology and processes are documented, but may or may not be tailored to each facet of the business. Results of Fraud Risk Assessments are communicated to senior leadership. There is a standardized scoring criteria to measure likelihood and impact. The Fraud Risk Assessment identifies significant risks using the fraud triangle and assesses the likelihood and impact and remediation activities.	Fraud Risk Assessments are conducted on a scheduled basis by a team of dedicated and experienced individuals that are well-versed in fraud risk management. Fraud Risk Assessment methodology and processes are formally documented and can be tailored to the organization's distinct operational business units. Standardized scoring criteria are consistently applied to assess the likelihood and impact of fraud risks. Management is comfortable that all known fraud risks currently facing the organization have been considered. Fraud risk tolerance is established and consider the balance between risk and reward. The results of the fraud risk assessment are compared to tolerance level Results of Fraud Risk Assessments are communicated to all applicable parties including management and Board leadership. Reporting contains actionable plans for fraud risk remediation.	Fraud Risk Assessments are conducted on a scheduled basis consistent with the organization's fraud risk appetite by a dedicated team of individuals with knowledge and experience in designing and assessing controls to mitigate fraud risks. Fraud Risk Assessment methodology and processes are documented in detail, and are comprehensive to encompass all facets of the organization's business. Results of the Fraud Risk Assessments are used in to improve processes and mitigate fraud risks on an ongoing basis. The connection between risk appetite, risk tolerance, and risk portfolio (likelihood and impact) is used in decision making so that priorities are aligned with strategic goals. Fraud Risk Assessments take into account emerging risks trending in the industry(s) the organization operations in. Process owners are involved in identification of risks, regularly reviewing and recommending fraud risk indicators

Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

COSO Category	1 - AD HOC	2 - INITIAL
Fraud Control Activities 	Process and control ownership is non-existent for the most part. In most cases process ownership is declared, and not appropriately assigned. The process and control owner does not understand the potential for fraud occurring in his or her purview. Fraud risk is not considered in the implementation of business process and IT controls. Fraud controls are not documented in any kind of narrative or risk and control matrix.	Organization has recognized the importance of implementing antifraud controls, but has not reached any level of maturity in implementing a robust antifraud control environment. Organization's existing antifraud controls are not consistent business practice, and lack rigor and discipline. Existing processes and antifraud controls are documented, but are not centralized and understood by all stakeholders.
Fraud Investigation & Corrective Action 	A formalized Fraud Investigation Unit is not established within the organization. Fraud investigation and mitigation is the sole responsibility of business line individuals. The organization does not have a process for reporting and investigating potentially fraudulent activity perpetrated by internal or external parties. The organization does not have a process for mitigating fraud events and implementing corrective actions to avoid future instances of the same or similar fraud schemes. Fraud investigation and mitigation processes are not documented.	A Fraud Investigation Unit is in place and operates according to documented policies and procedures. The organization has a reporting process for business line employees to communication suspicious behavior to the Fraud Investigation Unit, but the process may not be fully understood and utilized across the organization. The Fraud Investigation Unit conducts investigations and reports on their findings. Corrective actions are recommended, but may not always be implemented, or followed up on to ensure they have become consistent business practice.

Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

Strength Level

3 - REPEATABLE	4 - MANAGED	5 - LEADERSHIP
Organization has deployed both preventive and detective antifraud controls. Reporting structures to senior management and the Board of Directors when necessary has been formalized. Organization's processes and antifraud controls are established, understood, and consistently performed. Organization understands the importance of and has begun implementing data analytics processes to help them better understand fraudulent patterns and behaviors. Processes and antifraud controls are standardized and documented.	Organization has installed a combination of mature preventive and detective antifraud control activities by considering the results of the fraud risk assessment, organization and industry-specific factors. Organization has established data analytics capabilities in their antifraud processes to identify anomalous transactions. Predictive analytics on the horizon for the organization. Organization's processes and antifraud controls are thoroughly understood and documented in procedural narratives and/or risk and control matrices. Antifraud controls are incorporated into Internal Audit's planning and testing.	Organization has installed a combination of mature preventive and detective antifraud control activities by considering the results of the fraud risk assessment, organization and industry-specific factors. Organization has deployed a proactive, well-designed, and rigorous data analytics processes to detect anomalous transactions and can use this information in data analytics models to predict fraud patterns and prevent given fraud from occurring. Organization has implemented antifraud control activities are thoroughly understood and documented in procedural narratives and/or risk and control matrices. They are reviewed and revised on a consistent basis. Key fraud controls are tested by internal audit. Recommendations are implemented by management.
The Fraud Investigation Unit has a clearly defined purpose and role, that the organization understands. The organization has a documented reporting process for business line employees to communicate suspicious behavior to the Fraud Investigation Unit. The organization is fully aware of and uses this process. The Fraud Investigation Unit conducts investigations and reports on findings according to an established and repeatable process. Corrective actions are monitored to ensure they are adopted in process. The investigation unit reports to the board about the status of remediation of issues and control weaknesses.	The Fraud Investigation Unit has a clearly defined purpose and role, that the organization understands. The Fraud Investigation Unit team members complete training consistently. The organization has a documented reporting process for business line employees to communicate suspicious behavior to the Fraud Investigation Unit. The organization is fully aware of an uses this process. The Fraud Investigation Unit conducts investigations and reports on findings according to an established and repeatable process. Corrective actions are monitored to ensure they are adopted in process. The organization communicates a strong, consistent response to fraud incidents. The organization evaluates the investigative process to identify areas for improvement. Standardized scoring criteria is consistently applied to assess the likelihood and impact of fraud risks.	The Fraud Investigation Unit operates under established policies and procedures that are continuously evaluated for improvement. Fraud Investigation Unit team members take formal measures through consistently completing training, attending industry conferences, and independently researching to remain abreast of the changing fraud landscape. The organization has a reliable process and reporting tool for business line employees to communicate suspicious behavior or transactions. The Fraud Investigation Unit pushes out information to the business lines on continuous basis to alert them of new trends in the fraud landscape impacting their job responsibilities. The Fraud Investigation Unit conducts investigations according to an established methodology and process, reports findings to the applicable stakeholders, senior management and the Board. The organization confirms that remediation activities are adopted into practice by subsequently monitoring. Additionally, management monitors the efficiency and effectiveness of its investigative process.

Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

COSO Category	1 - AD HOC	2 - INITIAL
Fraud Monitoring Activities 	Organization does not select, develop, and perform ongoing evaluations of the effectiveness of the five principles of fraud risk management. Deficiencies in the Fraud Risk Management Program are not identified in the periodic monitoring because there is no formalized Fraud Risk Management Program or monitoring activities. Fraud risk monitoring activities are not documented or are performed sporadically.	Organization has established monitoring controls, but they may not be consistently performed. Deficiencies discovered through monitoring activities may not have actionable solutions. A formalized escalation and remediation process may be nonexistent or immature. Existing monitoring activities are documented, but may not be understood by all stakeholders. Documentation may exist in different parts of the organization that is not standardized.

Appendix A: Enterprise Anti-Fraud Maturity Assessment Model©

Strength Level

3 - REPEATABLE	4 - MANAGED	5 - LEADERSHIP
Organization has repeatable monitoring activities in place and preforms them on a consistent basis. Organization has developed a formalized escalation and remediation process that is understood throughout the organization. Upward reporting to senior management and the Board is performed on major deficiencies. Monitoring activities are thoroughly documented and are consistent across business lines where possible. Monitoring activities such as data analytics are employed to assess the effectiveness of fraud control activities.	Organization consistently performs ongoing and ad hoc monitoring of its antifraud controls and processes, and has an established reporting structure for alerting senior management and the Board when processes or controls are ineffective. Monitoring activities effectively identify deficiencies and considers known fraud schemes. The organization makes an effort to stay abreast of new schemes. Communication and remediation processes are established and performed. The methodology for periodic and ongoing monitoring is thoroughly documented and understood throughout the organization. The organization has established criteria to measure the effectiveness of their fraud risk management program such as extent of loss, number of hotline tips, length until detection, etc.	Organization consistently performs ongoing and ad hoc monitoring of its antifraud controls and processes, and has an established reporting structure for alerting senior management and the Board when processes or controls are ineffective. Organization periodically evaluates ways to improve monitoring. Monitoring activities effectively identify deficiencies and consider known fraud schemes and changes in the operating environment as well as emerging trends in the fraud landscape for the industry. The results of the monitoring activities are measured appropriately and any deficiencies are communicated and remediated timely, and according to established procedure. The methodology for periodic and ongoing monitoring is thoroughly documented and understood throughout the organization. Documentation is periodically reviewed and revised when process improvements are identified.

Appendix B: Fraud Risk Map© Template

The table below shows the fraud risk map filled in with four hypothetical examples. Click here for an Excel file containing a fraud risk map template.

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.	• Any change to an employee's salary requires more than one level of approval
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.	• Payroll list is periodically reviewed for duplicate or missing Social Security Numbers (SSNs), home addresses or telephone numbers • Appropriate forms are completed and signed by the employee to authorize payroll deduction and withholding exemptions
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.	• Employees are required to submit detailed expense reports containing receipts, explanations, amounts, etc. • Supervisors are required to review and approve all reimbursement requests
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.	• Spending limits are in place to limit expenses on hotels, meals, etc. • Supervisors are required to review and approve all reimbursement requests

Appendix C: Implementation Checklists

This appendix provides each checklist in the playbook, broken out by phase and by play, for your reference and convenience. You can select the phase or play you would like to see from the list below, which will automatically navigate you to your selected phase or play.

Fraud Risk Governance

1. Understand Where You Are and Where You Want to Be
2. Create a Culture

Fraud Risk Assessment

3. Think Like a Fraudster
4. Discover What You Don't Know

Fraud Control Activities

5. Use Data to Uncover Fraud
6. Knowledge Is Power

Fraud Investigation and Corrective Action

7. Lay the Groundwork for Investigations
8. Conduct Investigations

Fraud Risk Management Monitoring Activities

9. Monitor Your Progress
10. Report on Your Progress

Appendix C: Implementation Checklists

Fraud Risk Governance

Play 1: Understand Where You Are and Where You Want to Be

- ☐ **Identify your current state.** Evaluate your organization's current anti-fraud efforts and identify your current state both overall and across each of the five FRM principles. You can leverage the Grant Thornton's Enterprise Anti-Fraud Maturity Assessment Model© and the ACFE's FRM Scorecards to assist in evaluating the current state of your FRM program and related activities (see Tip #1).

- ☐ **Identify your goal state.** Identify your organization's goal state both overall and across each of the five FRM principles.

- ☐ **Develop a comprehensive FRM strategy and roadmap.** Your strategy and roadmap should align to your vision and goal state, including both short- and long-term plans to achieve your goal state based on the gaps identified. You can do this by pinpointing and prioritizing the gaps between your current level of maturity and your goal state both overall and across each of the five FRM principles. For example, the ACFE's FRM Scorecards will highlight where current gaps are across each of the five principles.

Play 2: Create a Culture

- ☐ **Develop a comprehensive FRM policy.** There is not a one-size-fits-all FRM policy. The specific contents and language of your policy should be tailored to your organization's objectives, environment, and risk profile. The ACFE provides a sample fraud policy you can leverage as a foundation here.

- ☐ **Define roles and responsibilities for the FRM program.** The FRM roles and responsibilities of all personnel should be formally documented. This includes the board of directors, audit committee, senior management, business-enabling functions, risk and control personnel, legal and compliance personnel, and all other employees, as well as other parties interacting with your organization, such as contractors and customers.

- ☐ **Maintain and communicate a continuous focus on FRM.** This can be done in many ways, including:

  - » Implement an enterprise-wide mandatory fraud training. This type of training provides a consistent basis for fraud awareness throughout the organization, which is a fundamental pillar of any FRM effort.

  - » Embed periodic fraud awareness events to encourage discussion across all levels of your organization. For example, the ACFE hosts Fraud Week as a spearhead for building fraud awareness across the globe.

  - » Demonstrate FRM leadership. Executives should set an example by taking fraud matters seriously, adhering to controls and policies, and taking corrective action when others fail to do so.

- ☐ **Periodically assess the effectiveness of your organization's fraud awareness efforts and track progress or gaps over time.** This might include conducting an annual employee survey to assess how knowledgeable employees are about the FRM program covering topics such as: (1) employee knowledge of how to report ethical concerns or observed misconduct, (2) any observed misconduct (and whether such misconduct was reported), (3) the effectiveness of the organization's responses to verified or proven unethical behavior, and (4) employee ability to report unethical behavior or practice without the fear of retaliation.

- ☐ **Assess the effectiveness of the enterprise-wide mandatory fraud training** against the stated learning objectives using an established methodology, such as pre- and post-training surveys to compare the level of understanding of the skills and concepts before and after the seminar. Adjust the training approach and materials based on the results.

- ☐ **Adapt the enterprise-wide mandatory fraud training periodically** to address new fraud schemes, fraud risks, regulations, policies, etc.

Appendix C: Implementation Checklists

Fraud Risk Assessment

Play 3: Think Like a Fraudster

- ☐ **Determine how you want to break out your fraud risk map.** This can be by department, business function, etc. In line with guidance in the Guide, be sure to consider the entire enterprise and recognize that fraud can happen at any level or within any component of the organization. Further, ensure that the way you break out your fraud risk map aligns with how you plan to conduct your fraud risk assessment.

- ☐ **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. You can leverage Grant Thornton's Fraud Risk Map Template© and the ACFE's Risk Assessment and Follow-Up Action Templates to assist in developing a framework for your fraud risk map. While these resources can provide a useful starting point, you should tailor your fraud risk map to meet the needs and objectives of your FRM program and fraud risk assessment.

- ☐ **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. Key considerations include:

  - » **When identifying fraud schemes, do so in a group setting whenever possible.** Your efforts will benefit from conversations between relevant stakeholders who understand the functional area for which you are brainstorming fraud schemes.

  - » **Consider both the actor** (i.e., the perpetrator) and the **fraud risk entry points** (i.e., the function or process thatwhich 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.** For example, the ACFE's Fraud Tree outlines the complete classification of internal, or occupational, fraud, which you can use to identify any additional internal risks you mightay not have considered.

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

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

Play 4: Discover What You Don't Know

- ☐ **Establish the fraud risk assessment team**, including clearly defining the members' roles and responsibilities and ensuring that the appropriate levels of management are involved. This should be informed by the established FRM governance structure and roles and responsibilities (see Play 2).

- ☐ **Determine your starting place.** You can either implement an enterprise-wide fraud risk assessment or a targeted fraud risk assessment. It might be beneficial to forgo an enterprise-wide assessment and instead conduct a pilot in a particular area to start small. This approach will allow you to test your methodology and implement lessons learned as you expand your assessment across other areas of the business. Either way, ensure that your starting place aligns to the roadmap and strategy you developed in Play 1.

- ☐ **Identify all fraud schemes.** (See Play 3.)

- ☐ **Estimate the likelihood and impact of each fraud scheme.** If your organization already has likelihood and impact scales developed for other risk management efforts, you might be able to leverage those here for consistency and to ensure that the fraud risk assessment results can roll up across your organization. You might also want to assess fraud risks on an inherent and residual basis. If you choose to do this, the key to this being effective is stakeholder communication to ensure understanding of these terms. Without that understanding, the results will not be insightful.

- ☐ **Identify existing fraud controls and their effectiveness.** Organizations usually have existing controls in place that serve as preventive or detective fraud control activities. As part of the fraud risk assessment process, the risk assessment team examines each specific fraud scheme or risk and identifies the existing related control activities. In some cases, there might be several existing controls. In other cases, the risk assessment team might conclude that no controls exist. After identifying existing control activities, the risk assessment team evaluates how effective these existing fraud control activities are in terms of mitigating fraud risk.

- ☐ **Prioritize fraud schemes.** Prioritizing risks will help you determine how to apply resources to effectively respond to the most important risks. In scoring and prioritizing risks, the risk assessment team should use the likelihood and impact assessments, as well as the presence and effectiveness of related control activities. For example, if a fraud risk lacks effective controls, it would be scored as a higher priority or a more significant risk than one with multiple effective controls in place.

- ☐ **Assess and respond to high priority or significant fraud schemes.** You may choose to strengthen existing control activities, add control activities, or consider using data analytics to combat high-priority or significant risks identified. Either way, the chosen response should align with your organization's fraud risk tolerance (see Chapter 2 of the Guide for details on developing your fraud risk tolerance) and the roadmap and strategy you developed in Play 1.

- ☐ **Document the risk assessment.** This can be done in a number of ways, but key items to document include the methodology deployed, the assessment results, and the organization's response strategies.

- ☐ **Reassess periodically**, considering changes external to the organization, operational changes, and leadership changes.

Fraud Control Activities

Play 5: Use Data to Uncover Fraud

The following checklist provides a framework for implementing an anti-fraud analytics program. It is important to take an iterative approach to analytics, so you can ensure that tests are designed and validated carefully. Further, the implementation of analytics should align with your overall FRM roadmap and strategy (see Play 1). You will also need to determine who will be responsible for your anti-fraud analytics program, which should be informed by the established FRM governance structure and roles and responsibilities (see Play 2).

- ☐ **Design your analytics.** Map the prioritized fraud schemes identified through your fraud risk assessment (see Play 4) to potential data sources and assess availability of relevant data. Once data is identified and availability is confirmed, determine the analytic techniques and tests you wish to implement.

- ☐ **Collect the data.** Work with relevant stakeholders across your organization to collect data. As part of this process, you will need to extract, transform/normalize, and validate the data to ensure that it will provide meaningful results when analyzed (i.e., to avoid "garbage in, garbage out").

- ☐ **Execute your analytics techniques and tests.** As execution proceeds, iterate and modify based on the data received, data

quality, user feedback, and test results. This process will be ongoing and will require refining your models as needed to ensure the effectiveness of the techniques and the accuracy and relevance of the results.

- ☐ **Report your findings and observations to relevant stakeholders.** Reporting should be in line with the established FRM governance structure (see Play 2). For example, if a potential fraud event is uncovered, then it should be referred to your organization's investigative body as outlined in your fraud risk policy. However, reporting should not stop there. You should report on key outcomes to other relevant stakeholders to ensure your findings and observations inform the FRM program and lead to lessons-learned that can be incorporated to strengthen current controls and mitigating activ tive. For example, if your intended audience is senior leadership, then presenting your findings and recommendations in a visual manner and focusing on the most important items needed for decision-making may be best. However, if you are presenting to business unit stakeholders, then tailor the results to highlight the items that affect their day-to-day work or items that they have ownership of so that they are aware of their risks and can begin work on mitigating them.

- ☐ **Implement remediation and corrective actions activities** based on the response strategies identified through your fraud risk assessment (see Play 4) and the established FRM governance structure (see Play 2). For example, if your results indicate that one type of fraud is a significant concern, then that information should feed back into your fraud risk assessment results to inform the response strategy and risk prioritization. Remember, all remediation and corrective action should also align to your overall FRM strategy and your long-term goals and vision of your FRM program (see Play 1).

Play 6: Knowledge Is Power

- ☐ **Determine who is responsible for the development and oversight of the targeted role-based training program.** This should align to the established FRM governance structure (see Play 2) and should define roles and responsibilities across the monitoring process.

- ☐ **Determine where to focus your training efforts** based on the results of other FRM activities. For example, you might choose to focus on an area of the business with the highest level of fraud risk or the most significant control gaps as determined by your fraud risk assessment.

- ☐ **Develop your training materials.** Consider the training best practices noted in Figure 8. If you already have training content, determine how this can be enhanced or expanded upon for the area you are focusing on.

- ☐ **Deliver your targeted role-based training.**

Evaluate the effectiveness of the training and adapt it periodically. Following delivery, evaluate the effectiveness of your training using an established methodology and adapt the training periodically based on both the results of your evaluation and on any changes in organization's fraud risks or operations. You can leverage the processes you have in place for enterprise-wide anti-fraud training (see Play 2) to perform these steps for your targeted role-based training efforts as well.

Appendix C: Implementation Checklists

Fraud Investigation and Corrective Action

Play 7: Lay the Groundwork for Investigations

- ☐ **Establish enterprise-wide fraud investigation and response protocols.** These protocols should align with the established FRM governance structure (see Play 2), as they are important inputs to your organization's overall fraud response plan. In addition, these protocols should define roles and responsibilities across the investigative process, including who is responsible for conducting investigations.

- ☐ **Assess your organization's current reporting mechanisms.** Promoting and supporting open communication and tips is vital to ensuring the effectiveness of reporting mechanisms and is a key element of an effective anti-fraud culture (see Play 2). You should assess current mechanisms to determine if they are adequately marketed and effectively operating, as well as whether any additional mechanisms should be added. For example, ensuring that you market reporting mechanisms to both internal and external parties and ensuring that you have an established whistleblower protection program in place will enhance the effectiveness of your reporting mechanisms.

- ☐ **Establish communication channels and procedures.** Following the conclusion of an investigation, you should have a clear path for disseminating the results of investigations, as necessary, in line with your established FRM governance structure (see Play 2). Communication procedures should cover items such as closing the feedback loop with the reporting party (as applicable) and reporting lessons learned to relevant stakeholders to improve controls and processes in place.

- ☐ **Establish monitoring mechanisms to ensure implementation of corrective action following a fraud investigation.** Communicating the results is the first step. Ensuring that there are monitoring mechanisms in place to track progress on corrective actions following an investigation is key to closing identified control gaps.

- ☐ **Establish mechanisms to assess investigation performance.** Solicit objective feedback on the effectiveness of your investigations process, such as a formal procedure for initiating an anonymous survey.

Play 8: Conduct Investigations

The following checklist outlines high-level steps needed to conduct an investigation. However, this process should align with and be guided by your established investigation and response protocols (see Play 7). Planning is essential to an effective investigation; as such, the foundation of your investigation is rooted in your investigative work plan.

- ☐ **Develop the investigation work plan.** Your investigative work plan should define and assign each investigative task to the appropriate team member. The plan should prioritize tasks and should be iterative as the investigation is carried out based on facts uncovered.

- ☐ **Implement the investigative work plan.** As the work plan is implemented, consider changes based on the unique circumstances of the investigation. During this stage, the investigative team will gather evidence, perform analysis, conduct interviews, etc. The team will need to document and track information related to steps taken and information collected.

    - » If allegations are substantiated or appear as if they are likely to have occurred, the investigative team will need to evaluate the root cause.

Following the investigation, several steps should be implemented to close the loop, as defined in Play 7:

- ☐ **Communicate the results,** leveraging established communication channels and procedures.

- ☐ **Take corrective actions and monitor implementation,** leveraging established monitoring mechanisms to ensure effective implementation of corrective action following a fraud investigation.

- ☐ **Evaluate investigation performance,** leveraging established mechanisms for performance evaluation to solicit objective feedback.

Appendix C: Implementation Checklists

Fraud Risk Management Monitoring Activities

Play 9: Monitor Your Progress

- ☐ **Determine who is responsible for oversight of the monitoring and evaluation efforts.** This should align with the established FRM governance structure (see Play 2) and should define roles and responsibilities across the FRM monitoring process.
- ☐ **Determine the type of monitoring and evaluation activities you plan to implement,** ensuring that all components of your FRM program are covered. For example, you should:
  - » **Conduct periodic evaluations and reassessments** of the FRM program, including reassessing for each of the five principles outlined in the Guide. For this type of reassessment, you can leverage Grant Thornton's Enterprise Anti-fraud Maturity Assessment Model© and the ACFE's FRM Scorecards.
  - » **Implement ongoing evaluations for fraud control activities and fraud risk mitigation activities,** as identified and implemented as part of your fraud risk assessment (see Play 4). For example, you can leverage data analysis to identify exceptions or deviations from key processes related to control activities to determine if the control is operating properly.
- ☐ **Set the scope and frequency of monitoring and evaluation activities.** For example, if you plan to conduct targeted evaluations of your anti-fraud training initiatives, you may decide that this should occur ad hoc (frequency) and be focused specifically on each occurrence of a new training program or topic (scope).
- ☐ **Establish measurement criteria for selected monitoring and evaluation activities.** For example, your measurement criteria for investigative performance might be based on the evaluation results.
- ☐ **Perform both ongoing and separate monitoring and evaluation activities.**
- ☐ **Implement corrective actions based on the results of monitoring activities,** as needed. 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.

Play 10: Report on Your Progress

- ☐ **Determine target audiences.** You may develop different reports for your board of directors or senior leadership than you would for individual business units or functions. So, understanding who you plan to target will be key to developing the right messages.
- ☐ **Determine the frequency of reporting.** This may differ for different audiences. For example, you may report annually to senior leadership and quarterly to leadership within the FRM program.
- ☐ **Identify the key insights and accomplishments.** Consider key insights and accomplishments both across individual activities and at an aggregate level to identify trends, patterns, and other relevant data points to showcase the program's accomplishments and changes. Similar to monitoring, it is best to focus on measuring the outcomes of FRM activities rather than simply reviewing outputs.
- ☐ **Deliver your report** in line with established frequency of reporting.
- ☐ **Evaluate the effectiveness and impact of reporting** and make changes based on the results and feedback.
- ☐ **Iterate** based on established frequency of reporting.