ANTI-FRAUD BLUEPRINT

A Foundational Approach to Fraud Risk Management

ACFE
Association of Certified Fraud Examiners

Grant Thornton

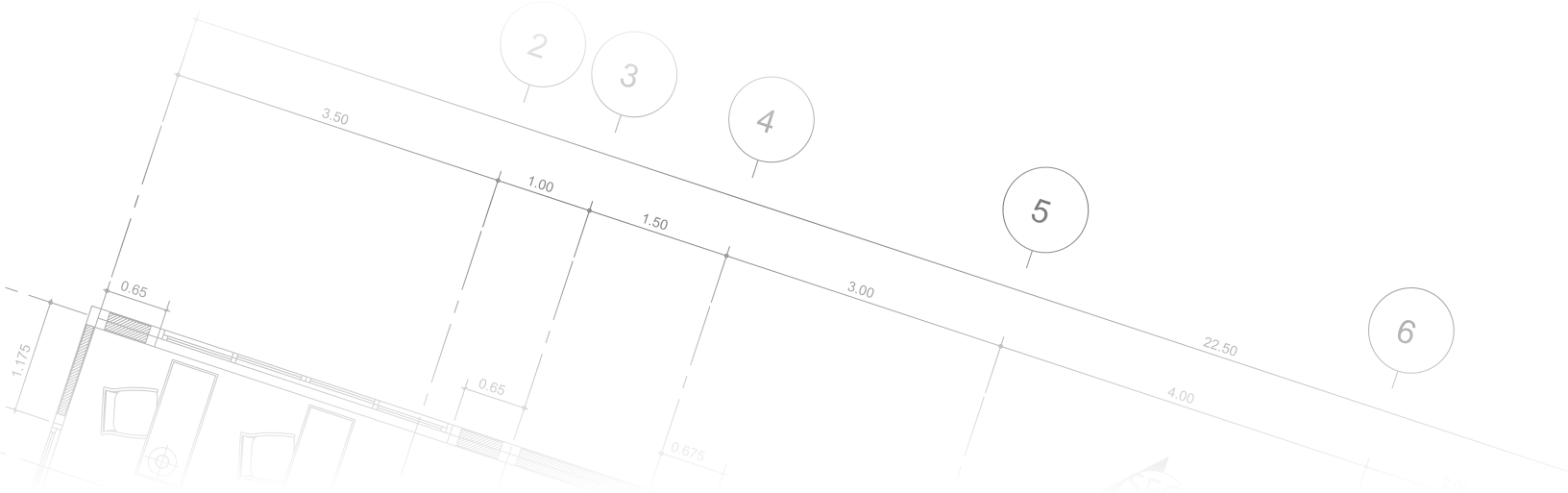
INTRODUCTION

Purpose and Background

In 2020, the Association of Certified Fraud Examiners (ACFE), in partnership with Grant Thornton, released the *Anti-Fraud Playbook* (Playbook), which provided easy-to-use, actionable guidance to help you fight fraud at your organization. The Playbook drew on insights from the first edition of the *Fraud Risk Management Guide*, issued by the ACFE and Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2016 (2016 Guide). The Playbook was intended to operationalize the concepts put forward in that 2016 Guide and leveraged the 2016 Guide's five Fraud Risk Management (FRM) principles to do so. The Playbook, and its ten "plays," proved to be a trusted resource for the organizations that leveraged it.

While the Playbook provided valuable guidance, substantial changes have taken place since it was published in 2020. For example, the COVID-19 pandemic dramatically expanded both the opportunities for and incidence of fraud worldwide, which served as a training ground for organized criminal groups in developing and perpetrating complex financial fraud schemes. In turn, the comprehensive *Fraud Risk Management Guide, Second Edition* was published by the ACFE and COSO in 2023 (2023 Guide), which updated the 2016 Guide to account for this changing landscape and to further align it to the COSO Internal Control Framework. More recently, artificial intelligence (AI) tools have become more widely available, which have intensified the speed and complexity of fraudulent activity, while also offering organizations powerful new capabilities to detect and prevent it. Even though the Playbook included valuable and actionable guidance on enhancing and evaluating FRM programs, organizations continued to find themselves struggling with where to start and how to adjust for this changing environment. As such, similar to how the 2016 Guide was updated by the 2023 Guide, it is necessary to now update the Playbook, and its ten tactical plays, with the expanded foundational guidance captured in this *Anti-Fraud Blueprint* (Blueprint).

Designed to align with the 2023 Guide, the intention behind the Blueprint is to help organizations build, mature, or enhance their FRM programs, as well as refresh the actionable guidance in the Playbook to reflect the changing fraud risk landscape.



The ACFE would like to thank Grant Thornton Advisors LLC for their partnership and expertise in creating this Blueprint. Readers are welcome to reach out to them at Zach.Snickles@us.gt.com *or* Paul.Avinger@us.gt.com *with any questions.*

How This Blueprint Is Organized

This document is designed to be the "Blueprint" behind the pillars of an effective FRM program, which align to the 2023 Guide's five Fraud Risk Management Principles (FRM Principles):

1. **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.
2. **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.
3. **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.
4. **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.
5. **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 Blueprint builds on these principles by providing practical guidance for getting started, as well as key questions and a checklist to consider along the way. It also highlights a subset of Points of Focus from the 2023 Guide, with an emphasis on those most relevant to the practical implementation of the concepts discussed in this document. Additionally, the Blueprint includes an updated **Enterprise Anti-Fraud Maturity Assessment Model©** that can be used to measure an organization's progress against the FRM Principles.

TABLE OF CONTENTS

FRAUD RISK MANAGEMENT PROGRAM OVERVIEW

What Is an FRM Program?

An FRM program is the set of people, processes, and technology through which the organization prevents, detects, and responds to fraud risk. It is the framework that defines how the organization safeguards its customers, assets, reputation, and the trust of its stakeholders. A well-designed FRM program enables leadership to understand fraud risk in a way that supports business objectives and fosters a culture of integrity.

At its core, an FRM program establishes accountability for fraud risk management by defining the roles and responsibilities of stakeholders, including leadership, business units, and the three lines of defense. Supporting components typically include a documented fraud risk management policy, targeted fraud prevention and detection controls, metrics, reporting and escalation protocols, feedback loops, awareness and training programs, and structured investigation processes.

An effective FRM program is tailored to the organization's size, complexity, and risk profile, yet flexible enough to adapt as risks, regulations, and technologies evolve. It provides the foundation for identifying inherent fraud risks, implementing effective controls, and embedding fraud awareness into business operations and decision-making. Ultimately, an FRM program demonstrates to team members, customers, regulators, and other stakeholders that the organization complies with expectations and is intentional about mitigating fraud.

Like the roof of a building that shields it from the elements, an FRM program protects the organization from fraud risks—and its strength depends on the integrity of the pillars that support it.

FIG. 1 Five FRM Principles

- Fraud Risk Governance
- Fraud Risk Assessment
- Fraud Control Activities
- Fraud Investigation and Corrective Action
- Fraud Risk Management Monitoring Activities

Integration with COSO and Enterprise Risk Management Frameworks

As mentioned in the Introduction, this Blueprint builds on the five FRM Principles described in the 2023 Guide, and those principles provide the structure for the subsequent sections of this document. The FRM Principles are themselves aligned to COSO's 2013 *Internal Control - Integrated Framework* (2013 Framework), which more broadly describes the components of an effective system of internal controls.

In addition to alignment with the 2013 Framework, the FRM program should be embedded within the organization's Enterprise Risk Management (ERM) and internal control environment to enable consistent oversight, reporting, and decision-making across risk domains. Integrating anti-fraud governance with ERM processes ensures that:

- Fraud risks are managed in concert with other operational and compliance risks and fit within enterprise risk taxonomies.
- Fraud control inventories leverage existing governance systems to support visibility and assurance activities.
- Fraud-related insights feed into strategic decision-making, resource allocation, and management reporting.

Integration with the broader ERM infrastructure strengthens the FRM program by treating fraud as a dynamic component of enterprise-wide resilience, rather than an isolated compliance issue. This is particularly important for large and complex organizations in which customer-facing teams bear much of the responsibility for directly managing fraud risks.

Regulatory and Audit Expectations

Regulators, auditors, and enforcement agencies increasingly expect organizations to demonstrate a proactive and documented approach to fraud risk management. Regulators across industries and jurisdictions emphasize the need for management and boards to understand and address fraud risk explicitly, as evidenced by a wave of published guidance and legislation in recent years.

A robust FRM program supports compliance with these expectations by providing:

- **A traceable line of accountability** from board oversight to operational controls
- **Evidence of continuous monitoring** and program improvement
- **A defensible framework** for demonstrating reasonable procedures and responsiveness when fraud incidents occur

An effective FRM program promotes transparency and accountability by linking day-to-day control activities to enterprise-level decision-making.

Whether your organization is establishing an FRM program for the first time or refining its program in response to an ever-evolving risk landscape, organizations need to assess where they are before they can figure out where they want to be. The updated **Enterprise Anti-Fraud Maturity Assessment Model©** developed by Grant Thornton can be used to determine the current and goal state of an enterprise's anti-fraud maturity in total and across each of the five FRM principles.

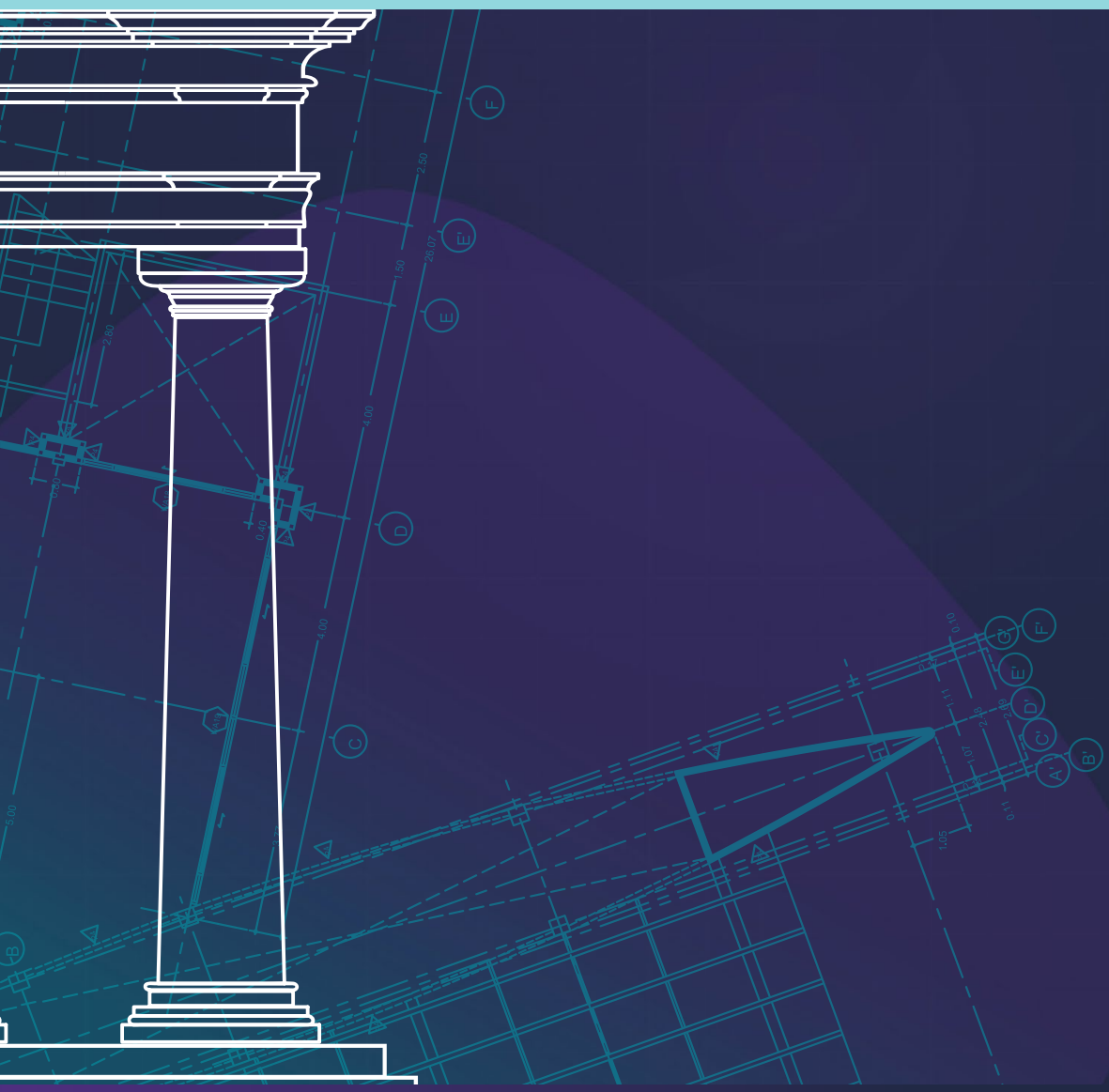
FIG. 2 Enterprise Anti-Fraud Maturity Assessment Model©

	AD HOC *LEVEL ONE*	INITIAL *LEVEL TWO*	REPEATABLE *LEVEL THREE*	MANAGED *LEVEL FOUR*	LEADERSHIP *LEVEL FIVE*
Fraud Risk Governance	• No documented fraud risk management policy exists and fraud risk activities are largely reactive. Awareness is limited and responsibilities are not defined or coordinated.	• Basic oversight exists but accountability is informal, inconsistent, and not well-understood across the organization. Governance activities occur inconsistently and are not centrally coordinated.	• A documented policy is in place and periodically updated. A governance structure with defined roles exists and senior leadership demonstrates visible support.	• Fraud risk management activities are embedded into business processes. Leadership actively oversees execution, and fraud governance is coordinated across functions.	• The organization continuously improves its fraud risk management program through benchmarking, lessons learned, and emerging risk insights. Leadership sets a strong tone and evaluates governance effectiveness regularly.
Fraud Risk Assessment	• A formal fraud risk assessment is not performed. Fraud risk exposures are addressed only after incidents occur.	• Fraud risks are identified informally through limited assessments, incident response, or interviews. Results are not comprehensive or consistently documented.	• A structured fraud risk assessment is conducted on a defined cycle and includes input across key areas of the organization.	• Assessment criteria are data-informed, updated for triggering events, and integrated with broader risk management processes. Risks are prioritized using consistent criteria.	• The organization dynamically reassesses risks using internal and external intelligence, trend analysis, and scenario testing, and uses results to guide proactive actions.
Fraud Control Activities	• Fraud controls are minimal, informal, or inconsistently applied, and primarily detective in nature.	• Foundational controls exist but roles, ownership, and documentation are limited. Controls vary by process or location.	• Preventive and detective fraud controls are designed, documented, and aligned to key fraud risks.	• Controls are routinely tested, automated where practical, and adjusted in response to identified issues or new risks.	• Control design leverages analytics, automation, and intelligence. The organization continuously evaluates control effectiveness and identifies emerging control opportunities.
Fraud Investigation and Corrective Action	• Investigations are informal and handled on a case-by-case basis without defined protocols or documentation.	• Basic reporting channels exist, but investigations vary in quality and timeliness. Corrective actions are inconsistently tracked.	• Investigation procedures, roles, and escalation criteria are defined, documented, and consistently applied.	• Case management tools, root-cause analysis, and corrective action tracking are used. Results are consistently applied across the organization.	• Investigations are timely, comprehensive, and consistently executed. Insights systematically inform fraud strategy, employee training, and enterprise risk management.
Fraud Risk Management Monitoring Activities	• Monitoring activities are limited and reporting is informal or event-driven.	• Metrics are tracked, but monitoring lacks structure, coverage, and defined thresholds.	• Standardized monitoring procedures exist and key metrics are routinely reported to management.	• Key risk and performance indicators are defined, compared to risk appetite/tolerance, and regularly reviewed by management.	• Continuous monitoring is in place. Insights from strategic decisions and reporting enable forward-looking risk management and program improvement.

FRAUD RISK GOVERNANCE

Effective fraud risk governance establishes the structure, authority, and expectations that guide how the organization manages fraud risk. Governance defines **who is responsible, how decisions are made, what standards apply, and how performance is measured**. Although the design of fraud risk governance should suit the needs of the organization's industry, size, and operating model, several foundational elements are consistent across leading programs:

- Clear organizational roles and responsibilities
- Formal governance policies and procedures
- Defined risk appetite supported by measurable tolerance thresholds



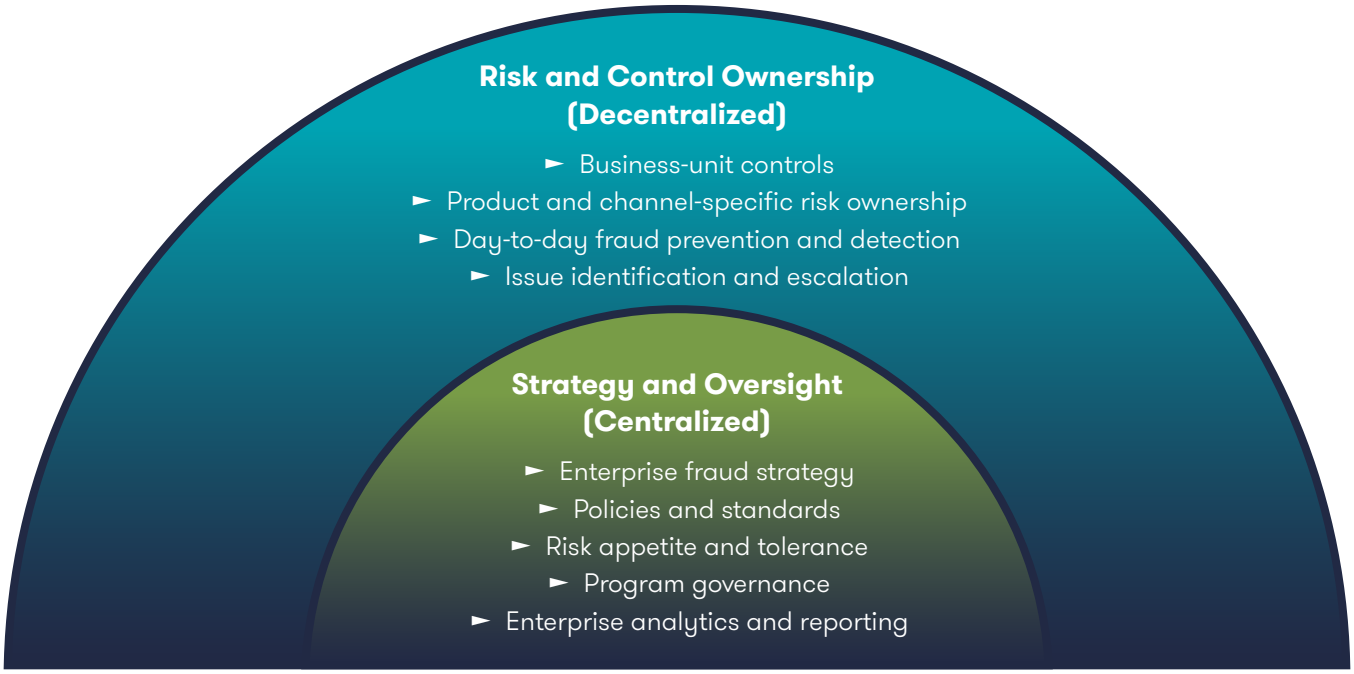
Organizational Structure, Roles, and Responsibilities

The structure of the FRM program should reflect the organization's needs, including the degree to which the FRM program is **centralized versus decentralized**. For example, some organizations may establish a centralized team with dedicated leadership to own the FRM program and lead strategy, risk assessment, analytics, and reporting for the enterprise. Other organizations may distribute those responsibilities across business units and control functions, coordinated through committees or shared frameworks.

It is helpful to consider centralization as a spectrum along two key dimensions:

- **Strategy and Oversight**: Responsibility for oversight, strategy, and standards—ranging from a strong central fraud risk management function to a more distributed governance model led by business units.
- **Risk and Control Ownership**: Responsibility for execution of fraud controls and the maintenance of risk registers—ranging from highly standardized enterprise-wide controls to processes specifically designed for products, services, or channels managed by operational teams.

FIG. 3 Example Fraud Risk Management Program Structure



In practice, most organizations find benefits in a hybrid framework with centralized strategy and oversight supported by decentralized, business-embedded risk and control ownership. This model allows the organization to maintain consistency in expectations, analytics, and reporting while ensuring that control design and day-to-day risk mitigation remain closely aligned to the operational contexts where fraud occurs. For many organizations, a centralized fraud team may be established to develop the enterprise-wide fraud risk profile, investigate reports from the first line, manage alerts from detective systems, and handle referrals to external parties (e.g., law enforcement, insurers, regulators).

Organizations should consider the Institute of Internal Auditors' (IIA) Three Lines Model of risk management as a basis for the roles and responsibilities for the FRM program. Under this model, the first line (business and operations) owns and manages risks generated by their activities; the second line (risk and compliance) provides oversight, challenge, and expertise; and the third line (internal audit) delivers independent assurance of the effectiveness of programs and controls.

Even with centralized coordination, fraud risk management is often inherently decentralized in execution. First line teams own the processes that generate fraud risk exposure and therefore play a critical role in identifying risks and implementing controls. Effective programs intentionally build **partnership mechanisms**, such as:

- Cross-functional fraud risk working groups (e.g., risk, compliance, anti-money laundering [AML], finance, cybersecurity, technology, business units)
- Shared case management systems, metrics, and dashboards
- Routine calibration sessions among business, risk, fraud, and analytics teams

The goal is not to push all activity to a central enterprise team, but to ensure that the enterprise and the business share ownership in a structured and transparent way.

Escalation Channels and Oversight Committees

Clear ownership and defined escalation pathways are essential to ensure that fraud risks are transparently managed and effectively overseen. Senior management and the board should have explicit responsibility for reviewing fraud risk exposures, evaluating the adequacy of controls, and overseeing response and remediation activities. Typically, this occurs through established governance committees (e.g., Board, Audit, or Risk Committee), which receive regular reporting on fraud trends, emerging risks, and the performance of the FRM program.

The organization should also maintain documented escalation protocols that outline when, how, and to whom fraud-related issues are raised. These protocols should cover:

- **Escalation of suspected or confirmed fraud events**, including investigation procedures and timely notification to appropriate oversight bodies and internal stakeholders
- **Escalation of operational risk or control breakdowns** that could create fraud risk exposure, even if fraud has not yet been detected
- **Escalation of risk measurement and monitoring results**, such as breaches of key risk indicator (KRI) thresholds, behavioral or transactional anomalies, or trends that indicate increased fraud risk

Escalation expectations should be defined at multiple levels of the organization—first line management, risk and control functions, and executive oversight—to ensure that emerging issues are surfaced early and evaluated consistently. This approach reinforces accountability, supports timely intervention, and strengthens enterprise-wide coordination in managing fraud risk.

Governance Documents

Governance is formalized through **policies, standards, and procedures** that define roles, expectations, and operating processes.

An FRM Policy should be more than a document on the shelf. It should enable execution by clarifying ownership, aligning roles and responsibilities, and reinforcing enterprise-wide accountability for preventing, detecting, and responding to fraud. A strong FRM policy typically includes:

- Definition of fraud and fraud-related misconduct
- Roles and responsibilities across the first, second, and third lines
- Requirements for fraud risk assessment and control evaluation
- Expectations for training and awareness
- Case reporting, investigation, remediation, and disciplinary processes
- Documentation and recordkeeping standards

With respect to procedures, the goal should be to embed anti-fraud controls and clear guidance within existing operational procedures for key processes (e.g., accounts payable). Other supporting procedures and guidelines specific to fraud risk may include process flows, escalation protocols, fraud detection playbooks, model governance standards, and corrective action frameworks.

FIG. 4 Hierarchy of Key Governance Documents

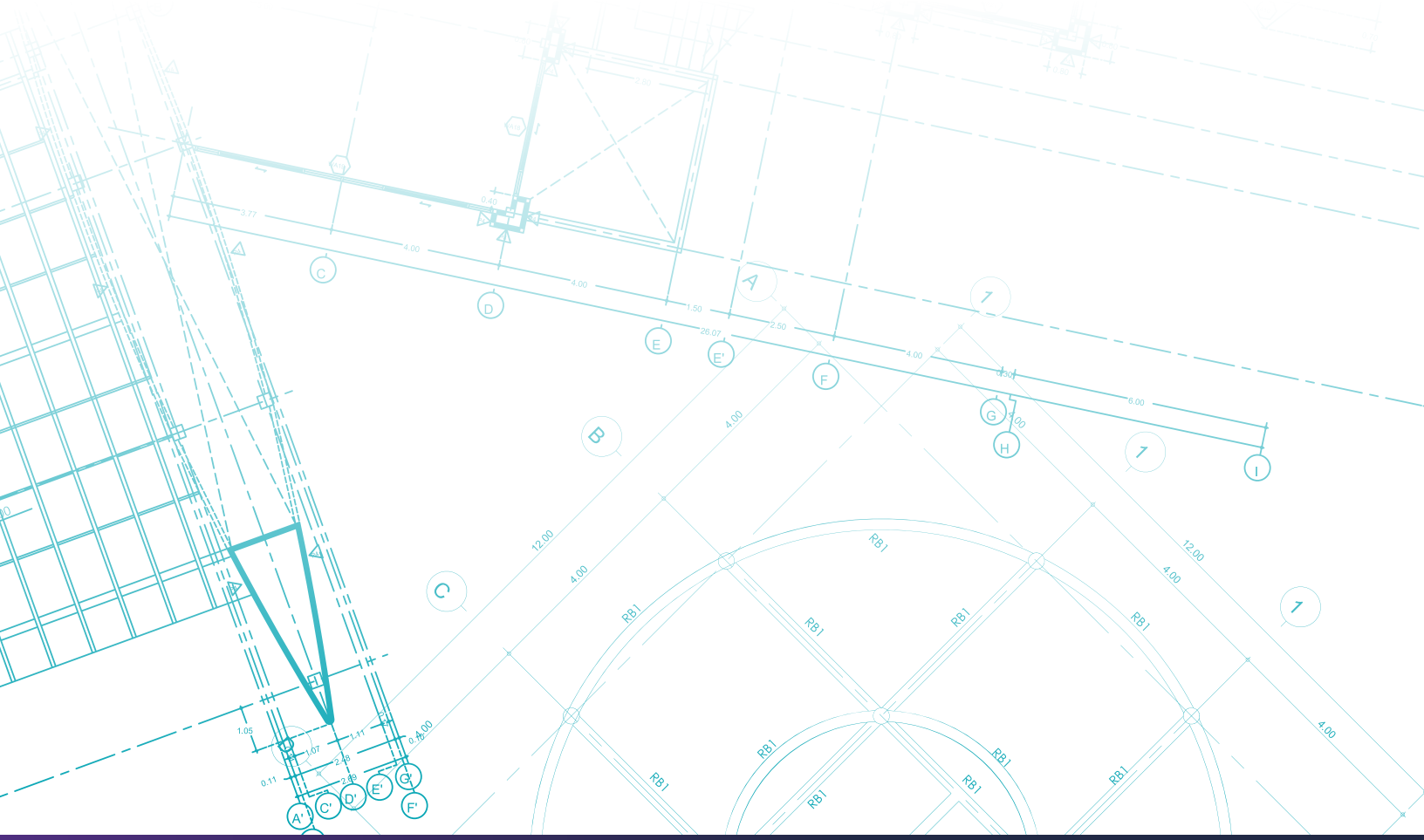
Risk Appetite and Fraud Tolerance

Fraud risk governance also requires clarity on **what level of fraud the organization is willing to accept**. This is expressed through statements of risk appetite, which should be approved by the board and aligned to the broader enterprise risk appetite.

Organizations should be realistic about the risk of fraud. A pragmatic FRM program does not attempt to eliminate fraud risk completely, but aims to reduce exposure and respond effectively. Fraud risk appetite is operationalized through metrics and **tolerance thresholds**, which set boundaries for measures such as:

- Fraud losses relative to revenue, customer type, or transaction volume
- Substantiated instances of fraud
- False positive rates in authentication or detective processes
- Case backlog and investigation timelines

Establishing fraud risk appetite and tolerance supports informed decision-making, resource allocation, and trade-off discussions between **customer experience, operational friction, and control effectiveness.**



Points of Focus

The following are selected points of focus from the 2023 Guide that pertain to the Fraud Risk Governance principle.

- Makes an Organizational Commitment to Fraud Risk Management
- Establishes a Comprehensive Fraud Risk Management Program
- Establishes Fraud Risk Governance Roles and Responsibilities Throughout the Organization
- Documents the Fraud Risk Management Program
- Communicates Fraud Risk Management at All Organizational Levels

Key Questions

- Do you have a comprehensive FRM policy in place?
- How is your FRM program integrated with your broader ERM program?
- Have you established, documented, and communicated roles and responsibilities related to FRM, including reporting mechanisms, across all levels of the organization?
- Is messaging about fraud risk management communicated throughout your organization, from leadership down to employees at all levels?
- Which stage outlined in the **Enterprise Anti-Fraud Maturity Assessment Model©** most closely aligns with the current state of your FRM program?
    - How does this vary across each of the five FRM Principles?
- What is the long-term vision for your FRM program? How clearly does this vision align with the organization's overall strategic objectives and its articulated risk appetite and tolerance for fraud?
- 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?

Checklist

- ✔ **Define and communicate a fraud risk appetite and tolerance statement**. Establish clear organizational expectations for acceptable fraud exposure (e.g., financial losses, regulatory violations, reputational harm) and tolerance thresholds that guide control investments, risk prioritization, and decision-making. This statement should be approved by executive leadership or the board, integrated into FRM planning and reporting, and revisited periodically as business and risk conditions change.
- ✔ **Conduct an Enterprise Anti-Fraud Maturity Assessment:**
  - **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 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.
  - **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.
- ✔ **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.
- ✔ **Refine roles and responsibilities for the FRM program**. Conduct a Responsible, Accountable, Consulted, and Informed (RACI) assessment to establish roles and responsibilities for key fraud risk activities. This helps define ownership across the business and encourages cross-functional involvement in fraud prevention (not just within business areas, but enterprise-wide).
- ✔ **Establish a defined response and notification plan for identified fraud risks**. The organization should document how fraud-related risks or trends will be addressed once identified, beyond simple escalation. This plan should outline response actions (e.g., strengthening controls, enhanced monitoring, communications) and criteria for when external notifications may be required (e.g., to affected customers). This plan should align with legal, compliance, and crisis/communications protocols, similar to how organizations maintain disaster recovery or incident response plans for cyber events.
- ✔ **Raise awareness of fraud risks, roles, and responsibilities throughout the organization. Executives should set an example by leading with ethics and integrity**, taking fraud matters seriously, adhering to controls and policies, and taking corrective action when others fail to do so. Implement a baseline enterprise-wide fraud training and identify key front line and operational teams who may need specialized training. Regularly update and adapt fraud training content to address new risks, technologies, regulations, and policies.

FRAUD RISK ASSESSMENT

A fraud risk assessment (FRA) is a structured process to identify where and how fraud could occur, evaluate the likelihood and impact of those risks, and prioritize actions to improve control effectiveness and reduce residual risk. It should be proportionate to the organization's size, complexity, and risk profile, and flexible enough to accommodate new products, services, channels, geographies, and partners. The goal is practical: Create a clear view of exposure and a forward-looking plan to strengthen prevention, detection, and response while upholding business performance.

Triggering Events

Determining when to conduct an FRA is as important as how it is performed. While many organizations follow a periodic cadence (e.g., annually or bi-annually), fraud risk exposure can shift dramatically based on changes to the organization, its products and services, and the external environment.

The organization should consider conducting an FRA in response to **triggering events** when they are meaningful or strategically important. Triggering events may involve major operational changes, new product launches, system implementations, or emerging fraud schemes that alter the organization's risk profile. For example:

- Mergers, acquisitions, or divestitures
- Entry into new markets, sectors, or geographies
- New products, services, channels, or business models
- Major technology changes (e.g., new platforms, AI features, payment channels, identity tools)
- Material changes in laws, regulations, or enforcement expectations
- Incidents, control failures, vendor changes, or audit/examination findings
- Significant shifts in customer demographics or behavior
- Macroeconomic or geopolitical developments

Assessment Scope

Organizations should clearly define the scope of what will be evaluated during the FRA. Depending on its size, structure, and risk profile, an FRA can be performed at a **broad enterprise level or targeted to specific business units, products, or processes** that present greater risk. Selecting the right scope requires understanding where fraud could most significantly impact the organization, including areas with high transaction volume, complex operations, sensitive data, or financial exposure.

Consider the operational characteristics of the organization's business that shape its exposure to fraud risk. For example, within the order-to-cash function, factors might include:

- **Front-end channel**: how the interaction starts (e.g., in-person, contact center, web, mobile app, kiosks, partner portals, API integrations, marketplaces)
- **Product or service**: what is being accessed or transacted (e.g., physical goods, digital content, claims/benefits, memberships, loyalty points, financing)
- **Customer type**: consumer, small business, commercial, government, vendor, or contractor
- **Payment type**: cash, card, invoice, ACH, wire transfer, P2P, wallets, credits, crypto/tokens, benefits-in-kind

Enterprise Factors

An effective FRA should evaluate the **enterprise-level factors** that drive fraud risk exposure. The industry or sector to which the organization belongs sets the stage and provides context for the fraud risk environment. Fraud manifests differently according to the organization's operating model and the products and services that it provides to customers. An enterprise-wide FRA should begin with a high-level analysis of where the organization fits in the broader picture of the industry, including its comparable peer groups.

FIG. 5 Potential Factors

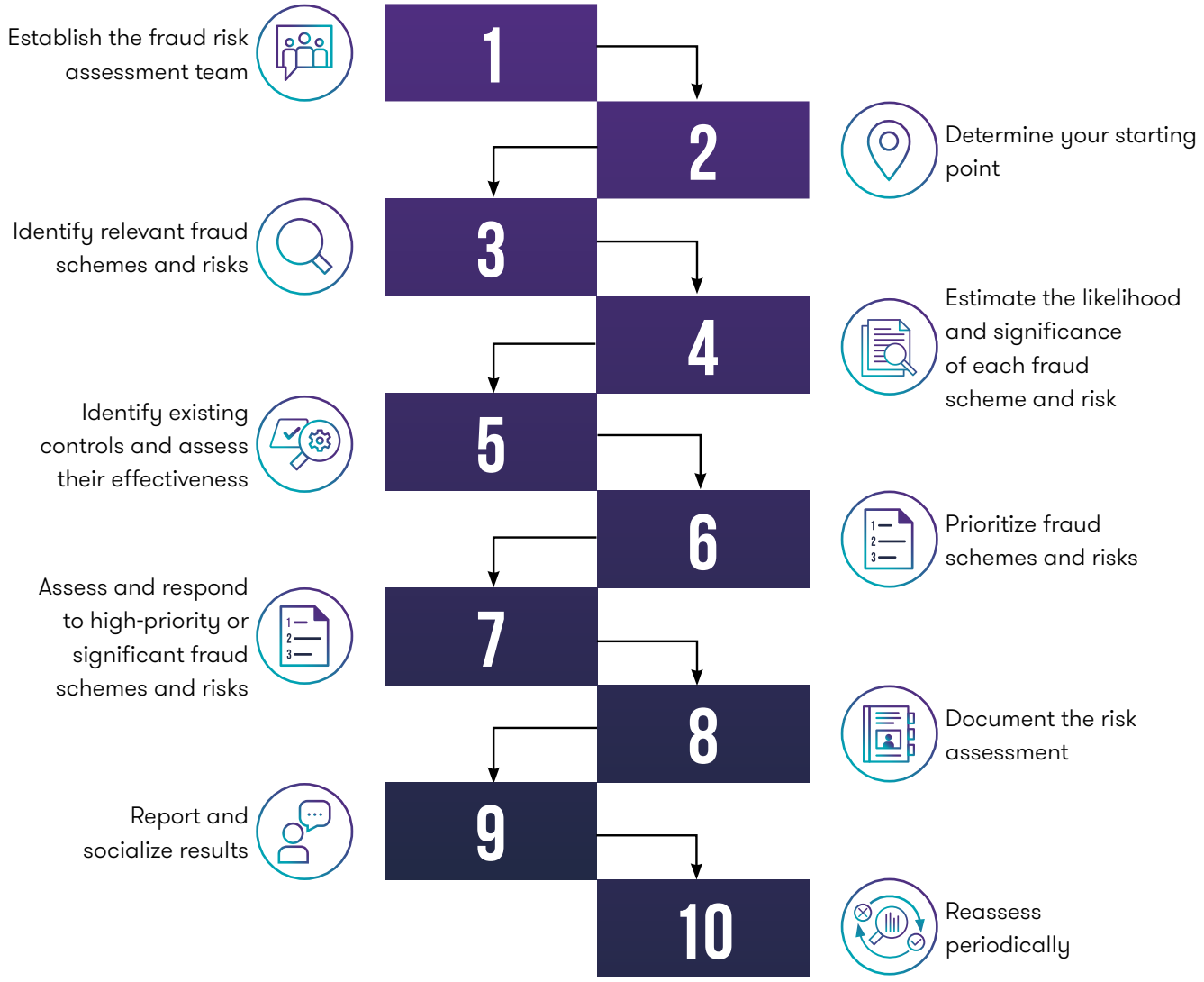
Customer Base	Geography	Third-Party Reliance
Customer types and segments: consumer, institutional, commercial	**Jurisdictional exposure:** laws, rules, regulations, sanctions, privacy	**Vendor and partner ecosystem:** contractors, agents, affiliates, platform providers
Exposure to higher-risk sectors: cash-intensive, high refund or chargeback rates, complex supply chains	**Cross-border operations:** shipping lanes, customs regimes, remote workforce footprints	**Technology and infrastructure partners:** identity, payments, cloud, AI, machine learning
Behavioral factors: churn rates, authentication, reliance on support, vulnerability to social engineering or account takeover	**Regional fraud typologies:** identity theft, document forgery, social scams	**Contractual and oversight controls:** service-level agreements, audit rights, data management, termination triggers, breach requirements

Fraud Risk Assessment Overview

The FRA process should be practical, iterative, and informed by the organization's fraud risk governance framework. Executing a successful FRA requires engaging the right stakeholders, critically evaluating risk exposure based on likelihood and significance, and documenting the results in a clear and effective way.

The following step-by-step process provides a practical framework for conducting a comprehensive assessment—from assembling the right team to evaluating, documenting, and continuously updating the organization's understanding of its fraud risk landscape.

FIG. 6 Steps of a Fraud Risk Assessment



Reporting the results of the FRA is a critical step in turning analysis into action. The findings should be summarized in a way that provides leadership and key stakeholders with a clear understanding of the organization's fraud risk exposure, top risks, control effectiveness, and priority areas for improvement. Effective reporting provides insights to translate detailed assessment findings into actionable strategies for strengthening controls, governance, and accountability. Results should be tailored to the audience—executive briefings should be focused and impactful, while individual departments require a greater degree of detail. FRA reporting informs remediation efforts and serves as a foundation for ongoing risk appetite discussions, KRI development, and continuous improvement of the FRM program.

Points of Focus

The following are selected points of focus from the 2023 Guide that pertain to the Fraud Risk Assessment principle.

- Involves Appropriate Levels of Management
- Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels
- Analyzes Internal and External Factors
- Considers Various Types of Fraud
- Assesses the Likelihood and Significance of Risks Identified
- Considers the Fraud Triangle and Other Models to Evaluate the Landscape
- Identifies Existing Fraud Control Activities and Assesses Their Effectiveness
- Uses Data Analytics Techniques for Fraud Risk Assessment and Fraud Risk Responses
- Documents the Risk Assessment
- Performs Reassessments and Assesses Changes to Fraud Risk

Key Questions

- When will you perform a fraud risk assessment? What changes will initiate a refresh or targeted assessment?
- Who will be on your fraud risk assessment team? How will you define roles and responsibilities?
- To what extent will the assessment leverage quantitative vs. qualitative inputs?
- Does your organization leverage standard rating scales, terminology, or methodologies for likelihood and impact? If not, how will you define ratings (e.g., high, medium, low)?
- What types of fraud are most prevalent based on known industry trends and past events? What other internal data can you leverage to identify potential fraud schemes?
- How might a bad actor exploit weaknesses in the organization's internal controls?
    - Who is incentivized to commit fraud?
    - Which types of customers, transactions, and channels pose the greatest fraud risk? Why?
    - What type of external and internal fraud schemes is your organization vulnerable to?
    - Have you considered non-financial fraud risks and schemes?
- How will you document the assessment (e.g., executive presentation, narrative, fraud risk map)?
- Who are the key stakeholders, decision-makers, or target audience for assessment results?

Checklist

- ✔ **Determine what is considered a triggering event.** Determining when to conduct an FRA is as important as how it is performed and should be customized for your organization.
- ✔ **Establish the fraud risk assessment team**. Define roles, responsibilities, and representation across management levels and key organizational components, consistent with the FRM governance structure.
- ✔ **Determine your starting point**. Analyze where roles, access, or responsibilities may create opportunities for fraud to occur. Consider the elements of the fraud triangle—pressure, opportunity, and rationalization—to understand behavioral and environmental factors that could influence misconduct.
- ✔ **"Think like a fraudster" to identify relevant fraud schemes and risks**. Identify both internal and external threats and think broadly across products, services, channels, customers, and geographies. Use data from investigations, loss events, audits, and known industry trends to ensure coverage of known schemes, while also brainstorming emerging or less-documented fraud scenarios unique to the organization's business model.
- ✔ **Estimate the likelihood and significance of each fraud scheme and risk**. If your organization already has likelihood and impact scales developed for other risk management efforts, consider leveraging those for consistency. Start with an assessment of fraud risks on an inherent basis, absent mitigating controls.
- ✔ **Identify existing controls and assess their effectiveness**. Align each identified scheme to its corresponding preventative and detective controls, evaluate their design and operating effectiveness, and determine whether any gaps, overlaps, or control weaknesses exist. This may include reviewing control data and documentation and gathering input from control owners to assess whether the controls are functioning as intended and aligned with the organization's current fraud exposure.
- ✔ **Prioritize fraud schemes and risks**. Prioritize risks based on likelihood, impact, and control effectiveness. Leverage insights gained from assessing inherent risk and control effectiveness to identify the residual risk of each scheme. Schemes with higher residual risks may indicate the need for corrective action and should be prioritized for further evaluation.
- ✔ **Assess and respond to high-priority or significant fraud schemes and risks**. Focus resources on high-priority schemes and strengthen or add controls, adjust processes, or apply analytics to address identified gaps. Document planned mitigation actions and monitor progress.
- ✔ **Document the risk assessment**. Capture the methodology, participants, assessment results, key risks, and response strategies. Maintain documentation at a level sufficient for transparency and repeatability.
- ✔ **Report and socialize results**. Communicate the results of the fraud risk assessment with the appropriate management teams, incorporating feedback that addresses high risk areas. Ensure all feedback is tailored to the relevant business units and clearly identify risks that warrant additional action or ongoing monitoring.
- ✔ **Reassess periodically**. Establish a cadence and identify key events that trigger the need for an updated fraud risk assessment. For example, some organizations may complete a fraud risk assessment biennially, or in response to a fraud event or the rollout of a new product/service.
- ✔ **Develop your fraud risk map**. Organize identified fraud risks by department, function, or another logical structure that aligns with your organization. Ensure coverage across the enterprise, recognizing that fraud can occur at any level or business component. Consider leveraging frameworks such as the ACFE's Risk Assessment and Follow-Up Action Templates as a starting point, tailoring them to your organization's needs and risk profile.

FRAUD CONTROL ACTIVITIES

Fraud control activities are the preventive and detective measures that the organization maintains to reduce the likelihood that fraud will occur and to detect fraud in time to limit harm. The objective is to create a coherent control environment that deters misconduct, protects stakeholder trust, and supports reliable operations.

Fraud Controls and Enterprise Risk Management

Fraud controls should be integrated with the broader Enterprise Risk Management (ERM) program to enable consistent oversight, reporting, and decision-making across risk domains. The organization should define the overarching risk management framework, including a description of fraud risk as it relates to other types of operational and compliance risk. Where possible, the FRM program should leverage control terminology, assessment criteria, and measurement scales consistent with other risk management programs.

By aligning fraud management activities with ERM principles, organizations can create a unified framework that supports proactive risk management and improves control effectiveness.

Fraud Control Registers

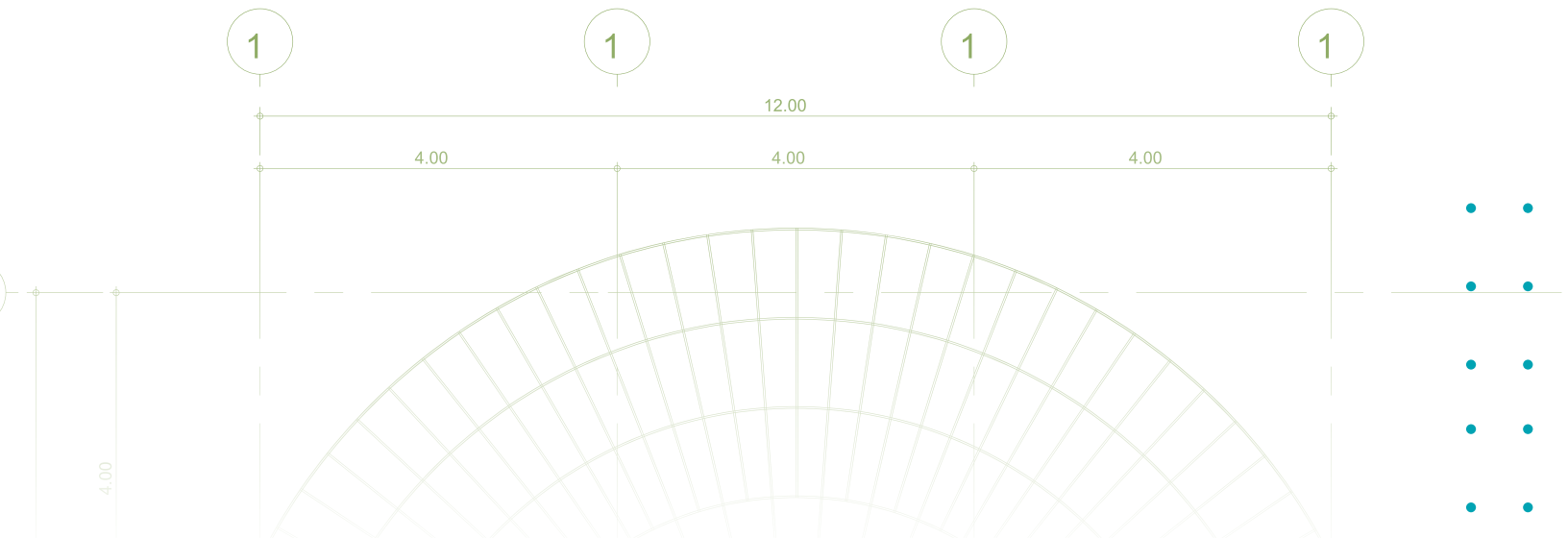
The organization should aim to develop a comprehensive register of control activities that support the FRM program **(fraud control register)**. Where appropriate, the fraud control register should reflect or align to fraud-related controls identified in other enterprise control registers, including operational, compliance, and financial controls. The fraud control register may be maintained centrally, even if the control owners are distributed in teams across the organization.

An effective control environment blends preventive and detective controls to achieve the right balance of fraud risk mitigation. Controls should be **tailored to the business context** by reflecting the organization's products/services, channels, processes, and data. One size does not fit all, and the strength of controls should match the risk involved in the process.

FIG. 7 Example Key Control Areas for Fraud Risk

- **Accounts Payable and Disbursements**: invoice processing, payment authorization, separation of duties, duplicate payment detection, and vendor payment controls
- **Vendor and Third-Party Management**: onboarding due diligence, sanctions screening, contract compliance, performance monitoring, and offboarding controls
- **Customer or Client Onboarding**: identity verification, eligibility validation, and periodic reassessments of customer status or risk indicators
- **Identity and Access Management**: authentication strength, privileged access controls, access reviews, session monitoring, and termination procedures
- **Monitoring and Detection Activities**: rules-based controls, analytics and model-driven detection, and exception reporting
- **Financial Reporting and Accounting**: journal entry approval, reconciliation procedures, variance analysis, and management review controls
- **Sales, Contracting, and Revenue Recognition**: pricing approvals, contract terms validation, revenue booking controls, and analysis of unusual sales patterns or concessions
- **Payroll and Workforce Administration**: employment verification, compensation approvals, timekeeping controls, and monitoring for fictitious or duplicate employee schemes
- **Inventory and Asset Management**: tracking of physical or digital assets, disposal controls, custody logs, and validation of asset transfers or write-offs
- **Expense Reimbursement and Procurement Cards**: spending limits, receipt validation, merchant category restrictions, and exception monitoring
- **System Configuration and Change Management**: logging of system changes, impact assessments, testing and approvals, and monitoring for unauthorized system modifications
- **Data Governance and Integrity Controls**: data quality validations, audit trails, anomaly monitoring, and safeguards against manipulation of key data elements
- **Incident Management and Reporting Channels**: whistleblower hotlines, fraud reporting protocols, triage criteria, escalation paths, and evidence retention

Fraud control registers should leverage existing governance systems to support transparency, accountability, and assurance activities. This integration ensures consistent ownership and makes it easier to evaluate whether fraud risk remains within tolerance.



AI and the Fraud Risk Landscape

Artificial intelligence (AI) and machine learning (ML) have dramatically reshaped the fraud risk landscape from both a risk and control perspective. Technology is accelerating how fraud is committed and transforming how organizations prevent, detect, and respond to emerging threats.

FIG. 8 AI's Role in Amplifying Fraud Risk Versus Strengthening Fraud Controls

IMPACT ON FRAUD RISKS

- **Volume and Scale**: Generative tools and automation can rapidly produce and deploy fraudulent attempts at massive scale, overwhelming defenses through sheer volume.
- **Customization**: AI-generated content—including voice, text, chat responses, and deepfake videos—make social engineering attempts (e.g., business email compromise, scam calls, impersonation attempts) more persuasive and tailored to their target.
- **Synthetic Media**: Deepfake audio, video, and images challenge traditional validation controls and increase risk for processes that rely on human recognition or trust-based verification.
- **Synthetic Identity**: Customer and third-party identities can be easily manufactured using a blend of compromised and fake data.

IMPACT ON FRAUD RISK MITIGATION

- **Advanced Detection and Pattern Recognition**: AI/ML improves detection by efficiently identifying complex patterns across large datasets and adjusting as fraud behaviors shift.
- **Real-Time Monitoring**: Behavioral, transactional, and contextual signals can be analyzed in real time and respond dynamically based on new patterns and user behavior.
- **Enhanced Identity Verification**: AI supports biometric verification, anomaly detection for images/documents, and behavioral authentication (e.g., typing, device hygiene).
- **Automation of Fraud Investigation and Response**: Case triage and root-cause analysis steps can be augmented to accelerate response and reduce workloads.
- **Threat Intelligence**: AI enables predictive modeling and scenario analysis to test emerging schemes, evaluate vulnerabilities, and proactively adjust.

AI can significantly enhance an organization's fraud defenses when thoughtfully implemented. Overall, fraud control activities are effective when they are risk-based, embedded in day-to-day processes, supported by policy and analytics, and governed through ERM and internal control structures.

Points of Focus

The following are selected points of focus from the 2023 Guide that pertain to the Fraud Control Activities principle.

- Integrates with the Fraud Risk Assessment
- Considers Organization-Specific Factors and Relevant Business Processes
- Considers the Application of Control Activities to Different Levels of the Organization
- Utilizes a Combination of Fraud Control Activities
- Uses Proactive Data Analytics Procedures
- Deploys Control Activities Through Policies and Procedures

Key Questions

- How can your FRM strategy guide the prioritization of fraud risks to target with analytics and detective controls?
- Who will be responsible for your fraud risk analytics program?
- What data is available related to the highest risk 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 will you implement? What resources and level of investment will be required?
- How will you integrate the design of fraud control activities with the fraud risk assessment?
- What fraud-related trainings do you already have in place? How can these be expanded upon or tailored to specific roles?
- What resources are available to help design your targeted and role-based anti-fraud training program?
- What information is available to help you determine your training needs, such as a fraud risk assessment or internal audit findings?
- Where is your organization particularly vulnerable to fraud? Which departments or groups within your organization have the lowest level of fraud awareness?
- Has your organization begun leveraging ML or Robotic Process Automation (RPA), and can it be utilized for fraud risk mitigation?

Checklist

- ✔ **Develop a fraud control activities register**. Create and maintain a centralized inventory of all fraud-related controls across the organization, regardless of where ownership resides. The register should document control objectives, control owners, frequency, level of automation, and evidence requirements, and should align with other enterprise control inventories (e.g., operational, compliance, financial).

- ✔ **Identify control automation opportunities**. Review whether high-risk or high-volume processes rely on manual controls that could be strengthened through automation. Identify areas where technology (e.g., workflow tools, data analytics, digital identity controls, or transaction monitoring rules) can replace or enhance manual checks.

- ✔ **Design your analytics**. Identify high-priority fraud risks and map them to available or potential data sources. Select analytic techniques appropriate for the scheme (e.g., rules-based queries, trend analysis, clustering, or supervised models). Ensure that the approach aligns with the fraud risk assessment and overall FRM strategy.

- ✔ **Collect and prepare the data**. Partner with relevant teams to obtain the data needed to perform analytics. Validate and prepare data so that it is structured, reliable, and suitable for analysis—recognizing that poor-quality data will limit effectiveness.

- ✔ **Report insights to relevant stakeholders**. Communicate results in a clear, actionable way that aligns with your organization's governance structure. Tailor reporting to the audience—concise summaries and trend insights for executives, and more detailed findings for operational teams responsible for follow-up.

- ✔ **Implement remediation and follow-up actions**. Use results to enhance fraud controls, policies, or monitoring practices. Prioritize actions based on impact and feasibility, and ensure accountability for remediation and ongoing ownership.

- ✔ **Develop targeted, role-based fraud training**. Tailor training to the specific responsibilities and fraud exposures of different roles (e.g., customer-facing teams, finance, technology, procurement). Where applicable, build on existing enterprise training and enhance content to reflect current fraud risks, emerging schemes, and lessons learned.

- ✔ **Evaluate and improve training regularly**. After rollout, monitor effectiveness through feedback, test results, performance indicators, or observed behaviors. Refresh and refine training as fraud risks evolve, new products launch, or organizational processes change.

- ✔ **Refresh internal audit's role in fraud control testing**. Internal audit should independently assess the design and operating effectiveness of fraud control activities, including both manual and automated controls. Internal audit testing results should feed back into control improvements, remediation planning, and ongoing monitoring of the FRM program.

FRAUD INVESTIGATION AND CORRECTIVE ACTION

A strong FRM program not only focuses on preventing and detecting fraud, but also ensures that suspected or confirmed fraud events are investigated consistently and resolved in an efficient and trustworthy manner. Fraud investigations serve multiple purposes: to determine what happened, identify responsible parties, assess control breakdowns, inform remediation efforts, and prevent reoccurrence. The organization's response to potential fraud events will drive the outcome of the case, as well as the trust of its team members, customers, and stakeholders.

Designing an End-to-End Investigations Process

Consistent with other aspects of the FRM program, the investigations process should be **tailored to the organization** and the subject matter being investigated. An effective fraud investigation and corrective action process provides a clear and timely pathway from allegation to resolution, supported by appropriate technology, governance, and documentation.

While the stages are often consistent—intake and triage, investigation, resolution, and follow-up—the specific workflows, roles, and tools may differ depending on whether the matter arises from a whistleblower hotline, a customer complaint or claim, a payment or transaction anomaly, or an internal control exception. Key design considerations include:

- **Standardized intake and triage**. Fraud-related matters should flow into a defined intake process. Triage criteria should categorize matters by severity, credibility, and potential impact, enabling the organization to route cases appropriately and prioritize cases that present greater financial, regulatory, or reputational risk.

- **Clear roles and responsibilities**. The process should specify the roles of teams that receive and log new matters, perform triage, lead investigations, and when other functions (e.g., human resources, technology, security, compliance, operations, legal) must be involved. These roles should align with the broader FRM governance model and the Three Lines Model of risk management.

- **Escalation criteria and decision points**. Investigations should include documented thresholds for escalation to senior management, risk or ethics committees, and the board. Examples include potential large financial losses, systemic control failures, matters involving senior personnel, or issues likely to attract regulatory or media scrutiny.

- **Engagement with legal**. Legal counsel should be involved when there is potential for litigation, regulatory exposure, labor implications, or concerns regarding attorney-client privilege. Legal advice must come from qualified legal professionals, and the FRM program should define when cases must be referred to counsel (e.g., matters involving senior leadership, potential criminal conduct, or multi-jurisdictional issues).

Investigations should follow a **risk-based approach**. For example, a low-impact customer complaint that is quickly resolved may require only limited review and documentation, while a whistleblower report alleging embezzlement will require a more robust investigative effort.

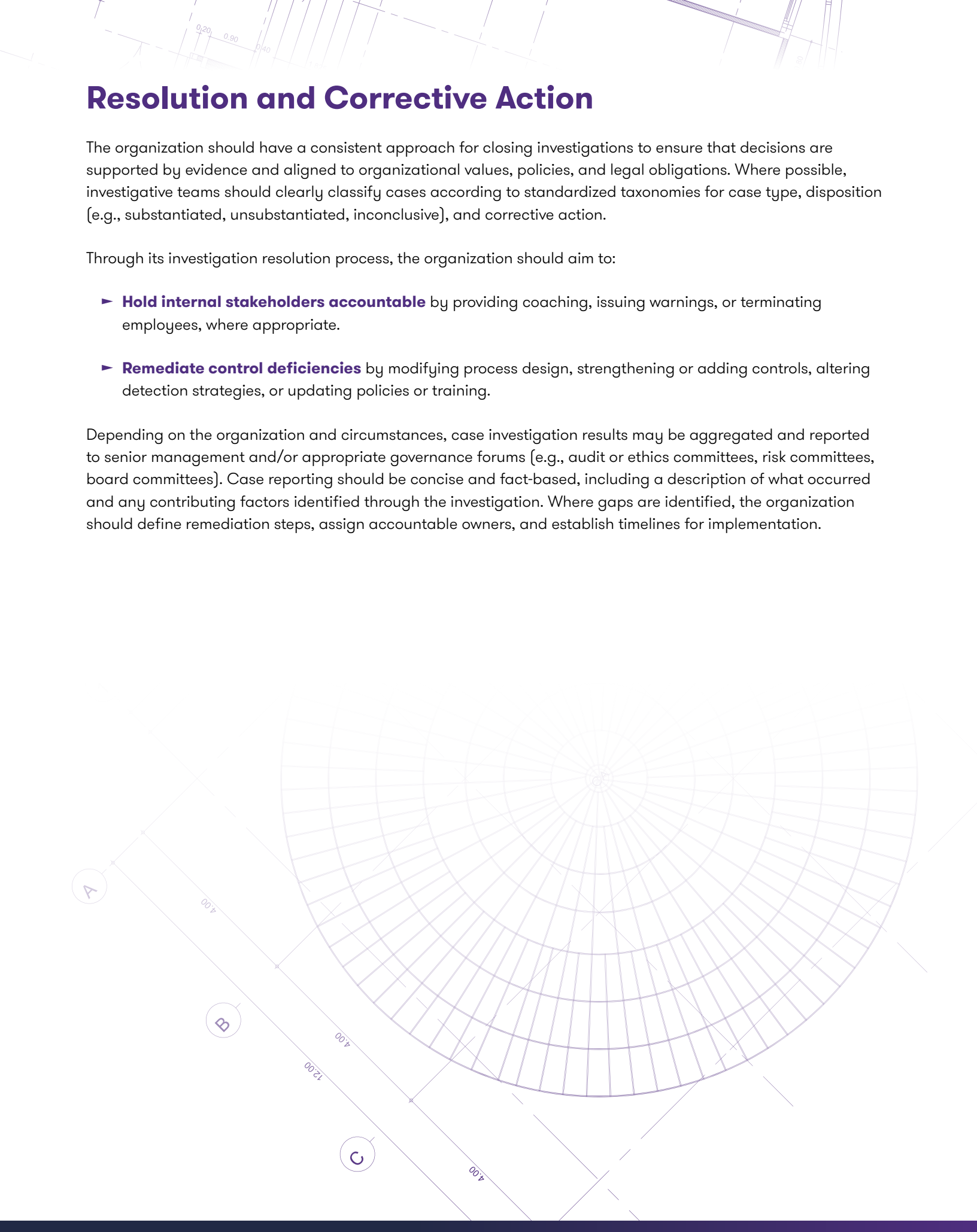
Resolution and Corrective Action

The organization should have a consistent approach for closing investigations to ensure that decisions are supported by evidence and aligned to organizational values, policies, and legal obligations. Where possible, investigative teams should clearly classify cases according to standardized taxonomies for case type, disposition (e.g., substantiated, unsubstantiated, inconclusive), and corrective action.

Through its investigation resolution process, the organization should aim to:

- **Hold internal stakeholders accountable** by providing coaching, issuing warnings, or terminating employees, where appropriate.
- **Remediate control deficiencies** by modifying process design, strengthening or adding controls, altering detection strategies, or updating policies or training.

Depending on the organization and circumstances, case investigation results may be aggregated and reported to senior management and/or appropriate governance forums (e.g., audit or ethics committees, risk committees, board committees). Case reporting should be concise and fact-based, including a description of what occurred and any contributing factors identified through the investigation. Where gaps are identified, the organization should define remediation steps, assign accountable owners, and establish timelines for implementation.



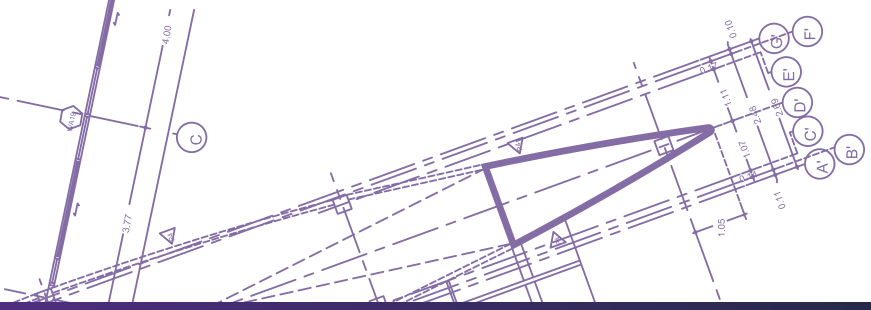
Points of Focus

The following are selected points of focus from the 2023 Guide that pertain to the Fraud Investigation and Corrective Action principle.

- Establishes an Effective Whistleblower Reporting System
- Establishes Fraud Investigation and Response Protocols
- Conducts Investigations
- Takes Corrective Action
- Evaluates Investigation Performance

Key Questions

- Does the organization maintain enterprise-wide governance documents that clearly define the process for intake, investigation, and response to fraud-related concerns?
- Who will be responsible for conducting fraud investigations? Does your organization have sufficient in-house resources to conduct these investigations?
- Are there mechanisms in place for employees to report allegations of fraud and misconduct (e.g., whistleblower hotline, online form)?
- Does your organization have a whistleblower protection program or non-retaliation policy in place?
- Does the organization categorize and route fraud risk cases to applicable teams based on severity, credibility, and potential impact?
- Are there tools or systems in place that facilitate the consistent documentation of fraud cases, investigations, and their outcomes?
- Are there any key performance indicators or mechanisms in place to measure the effectiveness of investigations and identify potential procedural enhancements or control gaps?
- Are there mechanisms in place to ensure lessons learned from fraud investigations are implemented into employee training and company procedures?
- Do you have a documented investigative work plan to guide each investigation? How might the work plan change from investigation to investigation?
- How does your organization determine accountability, remediation, asset recovery, or other activities to address the findings of an investigation?
- Does the investigation team have access to subject-matter experts if needed, including cybersecurity?
- What actions are taken upon the completion of an investigation, such as control enhancements, disciplinary action, or training? How is the appropriate action determined?



Checklist

- ✔ **Establish a comprehensive intake process**. Maintain clear, well-publicized channels for receiving concerns (e.g., whistleblower hotline, customer complaints, manager referrals) and record all cases in a centralized case management system.
- ✔ **Define enterprise-wide investigation and response protocols**. Document who investigates what, expected timelines, required documentation, and how matters are triaged based on risk (financial, regulatory, customer, or reputational).
- ✔ **Set escalation criteria**. Specify thresholds that trigger escalation to senior management, human resources, legal, or external parties (e.g., regulators or law enforcement), and ensure that these triggers are consistently applied.
- ✔ **Assess and maintain reporting mechanisms**. Periodically review the effectiveness of internal and external reporting channels to confirm they are accessible, trusted, and used appropriately.
- ✔ **Plan and conduct investigations proportionate to risk**. Assign qualified investigators, gather and preserve evidence, conduct interviews where appropriate, and document key decisions, while maintaining confidentiality.
- ✔ **Determine findings and root causes**. Conclude what occurred, who was involved, and which process, control, or cultural deficiency contributed to the issue.
- ✔ **Implement corrective and accountability measures**. Based on the facts and guidance from legal and HR, take proportionate actions such as control enhancements, process changes, training, restitution efforts, or disciplinary measures.
- ✔ **Track remediation and verify completion**. Monitor the status of agreed corrective actions, confirm they have been implemented, and evaluate whether they effectively address the root causes.
- ✔ **Evaluate investigation performance**. Periodically review investigation timeliness, quality, consistency, and outcomes to identify opportunities to improve procedures, tools, and training for the investigations function.

FRAUD RISK MANAGEMENT MONITORING ACTIVITIES

The FRM program is not a “set it and forget it” exercise. Once governance, assessment, control, and investigation processes are in place, the organization needs a disciplined approach to monitoring whether the FRM program is operating as intended and staying aligned to risk appetite. Monitoring activities provide ongoing insight into performance, emerging issues, and whether corrective actions are closing the gaps they were designed to address.

Objectives and Types of Monitoring

FRM monitoring activities should answer three questions:

1. **Is the program present and functioning?** (e.g., are required activities happening as planned?)
2. **Is it effective?** (e.g., are fraud risks staying within risk appetite and tolerance?)
3. **Is it improving over time?** (e.g., are key metrics stable or improving over recent periods?)

To achieve this, organizations generally use a mix of:

- **Ongoing monitoring**—built into day-to-day activities (e.g., management review of dashboards, periodic case reviews, model performance checks, oversight of key initiatives)
- **Separate evaluations**—periodic, more in-depth reviews (e.g., internal audit, independent testing, or third-party program assessments)

The mix and frequency should reflect the organization's size, complexity, and fraud risk profile.

Metrics, KRIs, and KPIs

A strong monitoring framework translates the FRM strategy into a **small, focused set of metrics**. These should be clearly defined, with data owners, calculation methods, and thresholds agreed upon in advance.

- **Key Risk Indicators (KRIs)** track changes in exposure and proximity to risk appetite. Examples include:
  - Fraud loss levels versus revenue, volume, or risk appetite thresholds
  - Rate of confirmed fraud events by product, channel, or customer segment
  - Volume and severity of fraud-related complaints, whistleblower reports, or investigation referrals
- **Key Performance Indicators (KPIs)** track how well the FRM program is functioning. Examples include:
  - Average time to triage, investigate, and resolve fraud cases
  - Completion rates for required anti-fraud training and role-based education
  - Completion and effectiveness of corrective actions

Metrics should be disaggregated where useful (e.g., by business line or geography) but remain **manageable and decision-oriented**.

Dashboards and Reporting

Depending on the organization's needs, monitoring results may be grouped into **tiered dashboards** and aligned with governance structures:

- **Operational dashboards** for fraud teams and business units provide detailed views to manage daily activity and resource allocation.
- **Management dashboards** for senior leaders summarize major trends, emerging issues, and status of key initiatives and corrective actions.
- **Board-level reporting** focuses on alignment with risk appetite, significant fraud events, systemic themes from investigations, and the overall maturity and resourcing of the FRM program.

Reporting frequency should be risk-based. Escalation triggers (e.g., exceeding fraud loss tolerances, significant control failures, or major incidents) should be clearly defined so that issues are rapidly elevated outside the normal reporting cycle.

Role of Internal Audit

Independent functions such as internal audit (and, where appropriate, external reviewers) should periodically assess whether:

- FRM monitoring activities are well-designed, properly executed, and based on reliable data.
- Metrics and reports provide an accurate and balanced view of the program.
- Prior findings and recommendations have been addressed in a timely and sustainable manner.

By combining clear metrics, disciplined reporting, and independent assurance, organizations can maintain a **holistic view of their FRM program's health**, demonstrate accountability to leadership and regulators, and support continuous improvement over time.

Points of Focus

The following are selected points of focus from the 2023 Guide that pertain to the Fraud Risk Management Monitoring Activities principle.

- Considers a Mix of Ongoing and Separate Evaluations
- Considers Factors for Setting the Scope and Frequency of Evaluations
- Establishes Appropriate Measurement Criteria
- Coordinates with Other Risk- and Compliance-Focused Functions in the Business
- Evaluates, Communicates, and Remediates Deficiencies
- Uses Data Analytics to Continuously Monitor and Improve

Key Questions

- Who will be responsible for conducting FRM monitoring activities?
- What ongoing or separate monitoring evaluations are key to assessing the performance and effectiveness of your FRM program?
- Will the use of internal audit or external third parties be necessary to conduct ongoing or ad hoc monitoring evaluations?
- How frequently should FRM monitoring activities be performed to align with your organization's size, complexity, and fraud risk profile?
- What factors may affect the scope of FRM monitoring activities? How might these changes affect scope or frequency of evaluations?
- What metrics and measurement criteria will be used to evaluate the FRM program?
- Who will be responsible for communicating the results of the FRM monitoring activities and how will they be shared with appropriate stakeholders?
- How will findings and deficiencies identified by FRM monitoring activities be escalated to the appropriate parties and remediated?

Checklist

- ✔ **Clarify oversight and accountability**. Confirm which committees, executives, and functional leaders are responsible for FRM monitoring. Align roles with the organization's governance structure and ensure that expectations are documented.
- ✔ **Define what will be monitored and how often**. Determine the scope of monitoring activities (e.g., program maturity, completion of required activities, KRIs/KPIs, control remediation progress) and establish a frequency (e.g., quarterly updates, annual program reviews, ad hoc evaluations following significant events).
- ✔ **Establish clear measurement criteria**. Set targets, thresholds, and indicators (e.g., loss trends, control failure rates, case closure timeliness, hotline usage trends, training completion, fraud exposure levels). Ensure that criteria support both performance evaluation and continuous improvement.
- ✔ **Perform ongoing and periodic evaluations**. Conduct routine monitoring (e.g., dashboard reviews, key results tracking) and periodic assessments (e.g., program maturity evaluations, benchmarking against industry trends or regulatory expectations).
- ✔ **Track corrective actions to closure**. Monitor remediation efforts related to fraud events, control gaps, and program weaknesses. Assign ownership, set due dates, and track progress until actions are completed.
- ✔ **Report meaningful insights to stakeholders**. Tailor reporting to the audience (e.g., board, senior leadership, business units). Focus on trends, emerging risks, and progress toward objectives—not just activity counts. Highlight areas requiring action or additional investment.
- ✔ **Use monitoring insights to strengthen the FRM program**. Incorporate lessons learned into fraud risk assessments, analytics priorities, control design, policies, and training. Update monitoring criteria as risks and business priorities evolve.

APPENDIX: ACFE TOOLS AND RESOURCES

APPENDIX: ACFE TOOLS AND RESOURCES

Fraud Risk Management Tools: Access these and other tools designed to accompany the ACFE/COSO Fraud Risk Management Guide at **ACFE.com/FraudRiskTools**.

ACFE and COSO Fraud Risk Management Guide

- Supplement the Anti-Fraud Blueprint with detailed guidance created by the ACFE and the Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- Access additional tools and resources.

ACFE's FRM Scorecards

- Evaluate your FRM program's current state for each of the five principles of fraud risk management.
- Identify maturity gaps and opportunities.
- Conduct periodic assessments.

Library of Anti-Fraud Data Analytics Tests

- Integrate data analytics tests into fraud risk assessment or investigative activities.
- Identify appropriate analytics tests based on specific schemes.

Sample Fraud Policies and Procedures

- Develop or update your fraud risk management policy.
- Assess and benchmark your procedures related to fraud risk management programs.

ADDITIONAL TOOLS AND RESOURCES:

Fraud Week

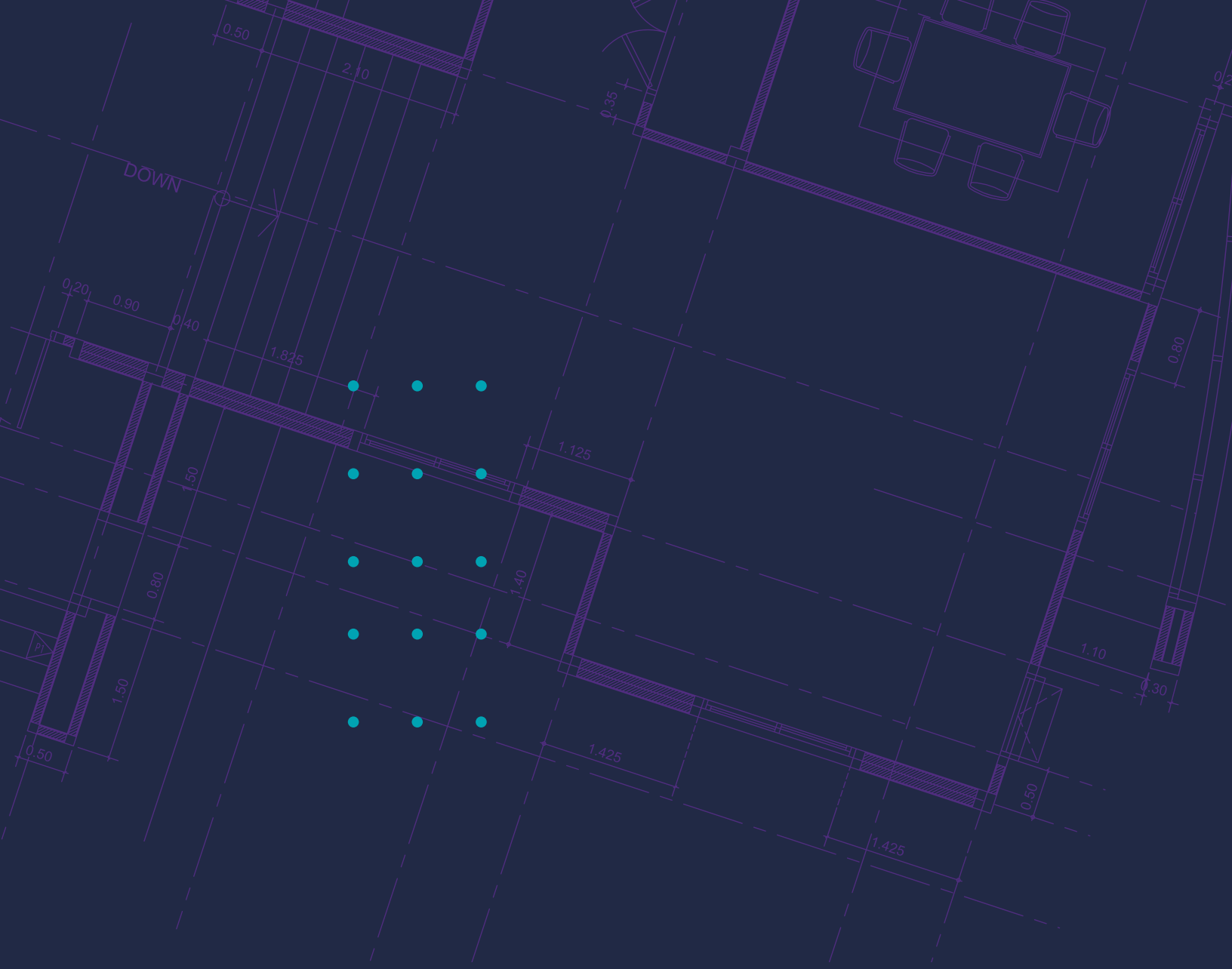
- Access resources to use in raising organizational fraud awareness.
- Establish the perception of detection in your organization—send a clear message that the organization takes fraud seriously and is actively monitoring for it.
- Become a sponsor of the world's largest fraud awareness campaign.

Fraud Tree

- Create, amend, or expand your organization's occupational fraud risk register.

ACFE's Report to the Nations

- Assess trends in occupational fraud as they relate to your organization's operations.
- Benchmark your control activities and evaluate opportunities for adjustments.



ACFE®
Association of Certified Fraud Examiners

Grant Thornton