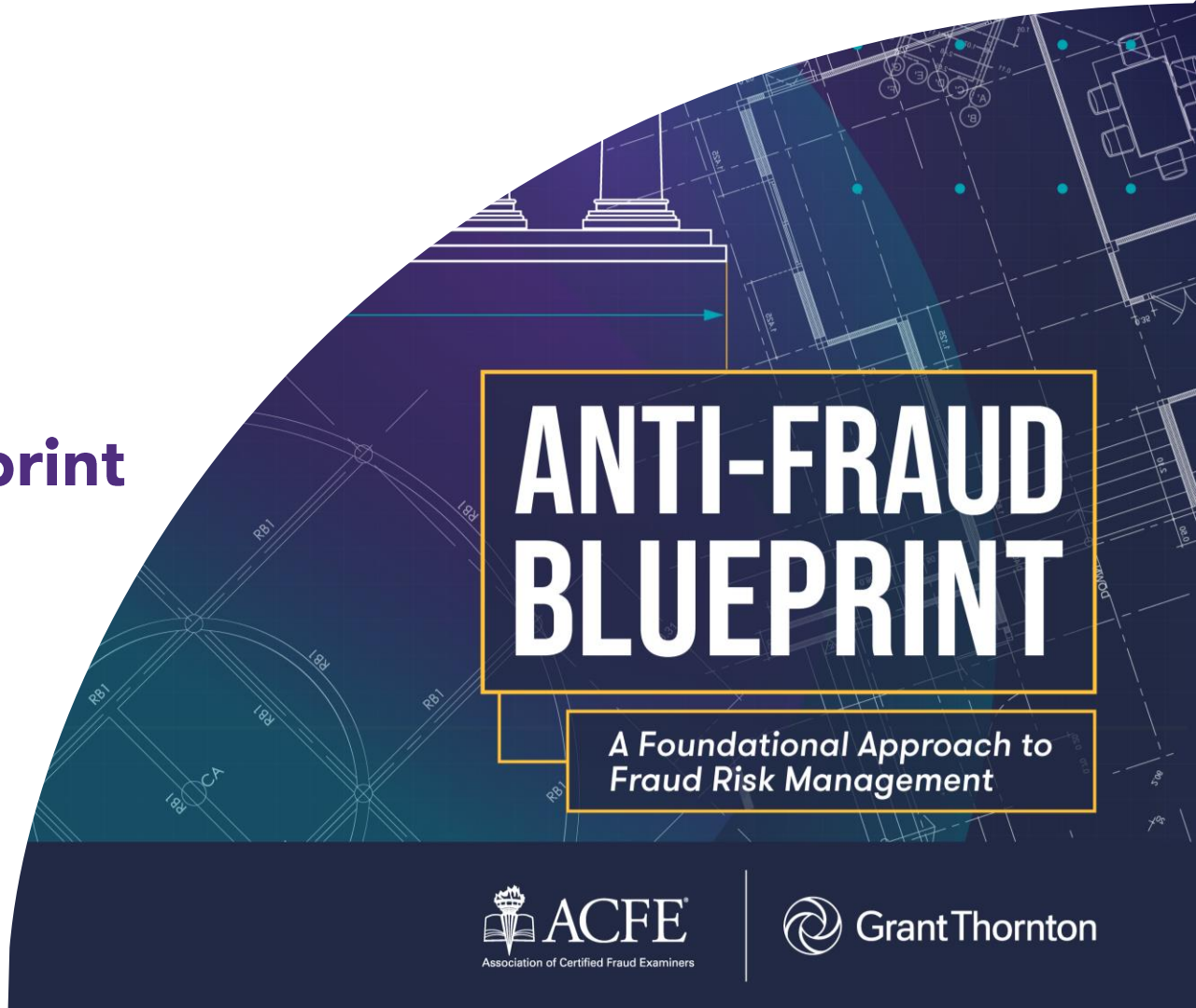
Grant Thornton

Anti-Fraud Blueprint

A Foundational Approach to Fraud Risk Management

IIA Atlanta Chapter

June 2026



Speakers

Zachary Snickles

Partner, Risk Advisory
Fraud Risk & Anti-Fraud
Grant Thornton Advisors LLC
Zach.Snickles@us.gt.com

Paul Avinger

Senior Manager, Risk Advisory
Fraud Risk & Anti-Fraud
Grant Thornton Advisors LLC
Paul.Avinger@us.gt.com

Learning Objectives

01 Articulate the purpose of a Fraud Risk Management program

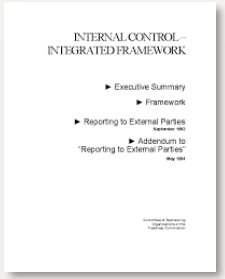
02 Distinguish between the five principles of fraud risk management

03 Describe the steps of a fraud risk assessment

04 Identify the stages of an Enterprise Anti-Fraud Maturity Assessment

Evolution of Fraud Risk Guidance

1992

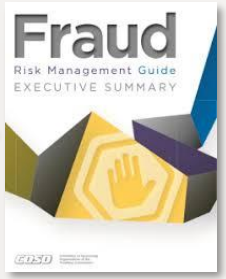


COSO releases its original Internal Control-Integrated Framework

2013

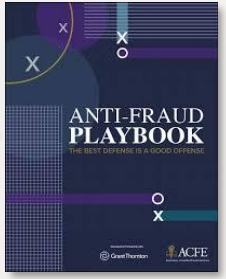
COSO incorporates 17 principles, including a new principle focused on fraud risk

2016



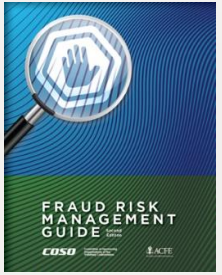
COSO & ACFE publish the Fraud Risk Management Guide, First Edition

2020



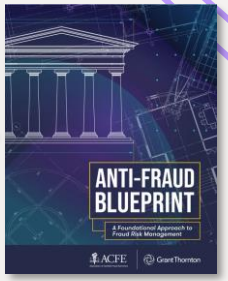
Grant Thornton & ACFE publish the Anti-Fraud Playbook

2023



COSO & ACFE publish Second Edition of the Fraud Risk Management Guide

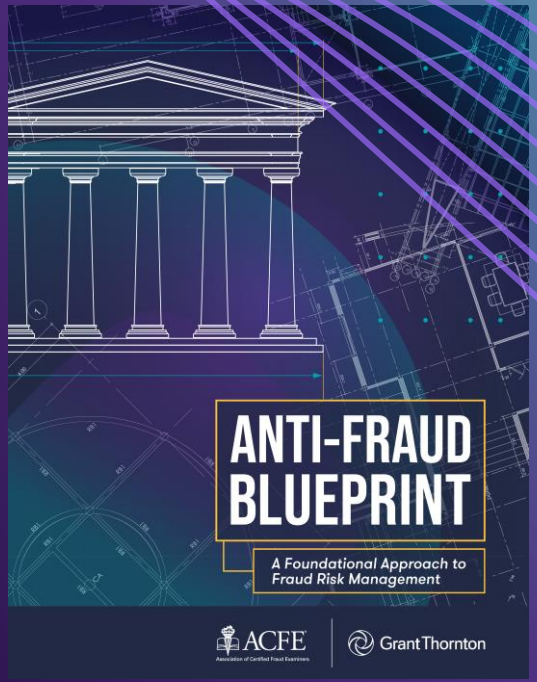
2026



Grant Thornton & ACFE publish the Anti-Fraud Blueprint

GT / ACFE Anti-Fraud Blueprint

- Developed in partnership with the Association of Certified Fraud Examiners (ACFE) to help organizations build, mature, or enhance their FRM programs
- Builds on the principles laid out in the 2023 second edition of the Fraud Risk Management Guide, issued by the ACFE and the Committee of Sponsoring Organizations of the Treadway Commission (COSO), by providing practical guidance for getting started and key questions to consider along the way
- Includes a streamlined Enterprise Anti-Fraud Maturity Assessment Model© that can be used to measure an organization's progress
- Addressed to anti-fraud leaders across industries
- Published February 12, 2026



Comprehensive Fraud Risk Management (FRM) Program

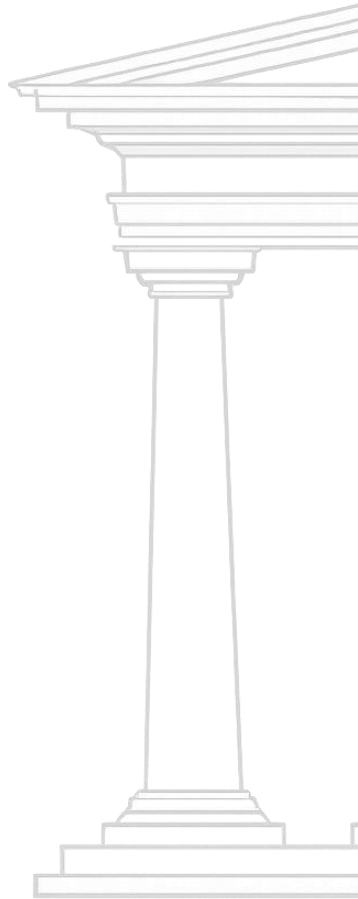
Principles from the *Fraud Risk Management Guide, Second Edition*, issued by COSO and the ACFE

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.

Grant Thornton

1. 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.



Organizational Structure, Roles, and Responsibilities

Fraud Risk Management Program Design

- The design of fraud risk governance should suit the needs of the organization's industry, size, and operating model.
- Leading programs tend to have:
  1. Clear organizational roles and responsibilities
  2. Formal governance policies and procedures
  3. Defined risk appetite supported by measurable tolerance thresholds
- 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.
- Clearly assign roles and responsibilities for:
  - Strategy and Oversight
  - Risk and Control Ownership

Example FRM Program Structure

Governance Documents

Governing documents include policies and procedures that **define the roles, expectations, and operating processes** within the organization.

FRM Policy Best Practices

- A FRM Policy is the foundation of a strong program and aligns teams to fraud risk management responsibilities, further strengthening accountability across teams.
- A strong FRM Policy should include:
  1. Definition of fraud and fraud-related misconduct
  2. Roles and responsibilities across the first, second, and third lines
  3. Requirements for fraud risk assessment and control evaluation
  4. Expectations for training and awareness
  5. Case reporting, investigation, remediation, and disciplinary processes
  6. Documentation and recordkeeping standards

Example Hierarchy of Governing Documents

Risk Appetite and Fraud Tolerance

Effective fraud risk governance considers the organizations risk appetite and tolerance while implementing practices that reduce exposure and respond to fraud risks.

- **Risk Appetite** is the amount of risk an organization is willing to accept to achieve its goals. It is the overall level of risk an organization is willing to take on and should be documented through formalized statements of risk appetite.
- Risk appetite is monitored through metrics and risk tolerance thresholds, which set the maximum risk an organization is willing to take on for each type of risk.
- Establishing **fraud risk appetite and tolerance** supports informed decision-making, resource allocation, and tradeoff discussions between customer experience, operational friction, and control effectiveness.

Example Fraud Related Metrics

- 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

Enterprise Anti-Fraud Maturity Model

The Enterprise Anti-Fraud Maturity Assessment Model was developed to provide clear guidance for organizations to assess the current state of their FRM programs and identify their desired goal state.

Fraud risk activities are informal, inconsistent, and carried out only in reaction to issues rather than through planned processes.

Basic fraud risk concepts exist but are fragmented and lack defined ownership, documentation, and standardized execution.

Core fraud risk processes are defined and can be performed consistently, though they remain procedural rather than fully integrated or governed.

Fraud risk management is structured, documented, and actively overseen with coordinated processes, monitoring, and governance.

Fraud risk capabilities are proactive, data-driven, and embedded across the organization, supported by strong tone-from-the-top and continuous improvement.

2. Fraud Risk Assessment

- A fraud risk assessment (FRA) is a structured process used to identify potential fraud risks, assess their likelihood and impact, and prioritize actions to enhance control effectiveness and reduce residual risk.
- The result of a FRA should be a clear view of exposure and a forward-looking plan to strengthen prevention, detection, and response while upholding business performance.

Triggering Events and Assessment Scope

An effective FRA should be proportionate to the organization's size, complexity, and risk profile, and flexible enough to accommodate new products, services, channels, geographies, and partners.

Triggering Events

Organizations should consider conducting an FRA in response to **triggering events** that alter the organization's risk profile. For example:

- Mergers, acquisitions, or divestiture
- 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

An FRA can be performed at a **broad enterprise level** or **targeted to specific business units, products, or processes** that present greater risk. 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. 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.

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

A fraud risk assessment is a structured process to identify where and how fraud can occur, evaluate the likelihood and impact of those risks, and prioritize actions to improve control effectiveness and reduce residual risk.

- **Goal**: To create a clear view of fraud risk exposure and an action plan that strengthens prevention, detection, and response while upholding business performance.
- **Reported Results**: Should be summarized to provide a transparent view of the organization's fraud risk exposure, top risks, control effectiveness, and priority areas for improvement. Results should be tailored to the intended audience:
  - **For organization leadership**: executive briefing that is focused on key findings and solutions.
  - **For individual business groups or departments**: additional detail to support remediation planning and execution.

3. Fraud Control Activities

- Fraud control activities are the preventative 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 Risk and Artificial Intelligence

As organizations are implement AI capabilities into their day-to-day operations, bad actors are using AI to develop sophisticated fraud attacks that circumvent the traditional anti-fraud controls. However, AI can significantly enhance an organization's fraud defenses when thoughtfully implemented.

Volume and Scale: Bad actors leverage automation to launch attacks at unprecedented speed and scale.

Customization: AI-generated, highly tailored messages enable more convincing and effective social-engineering schemes.

Synthetic Media: Deepfake audio, video, and imagery are increasingly used to bypass traditional authentication and verification controls

Synthetic Identity: Fabricated or manipulated identities are used to exploit onboarding, credit, and transaction processes.

Advanced Detection and Pattern Recognition: AI and machine learning enhance the ability to consistently identify fraud indicators, anomalies, and emerging patterns

Real-Time Monitoring: Continuous analysis of behavioral, transactional, and contextual data enables faster detection and response.

Enhanced Identity Verification: AI-enabled tools strengthen identity and document verification across customer and third-party interactions.

Automation of Fraud Investigation Response: Intelligent automation accelerates case triage, investigation workflows, and root-cause analysis

Threat Intelligence: Predictive modeling and scenario analysis improve foresight into emerging fraud risks and attack vectors

Fraud Control Activities

Fraud controls should be integrated with the broader Enterprise Risk Management (ERM) program to enable consistent oversight, reporting, and decision-making across risk domains. Organizations should aim to develop a comprehensive register of control activities that support the FRM program. An effective control environment blends preventative and detective controls to achieve the right balance of fraud risk mitigation.

The Role of Fraud Control Activities

- Ensures fraud risks are mitigated through a well-documented, actively managed set of control activities that are continuously enhanced and automated where feasible.
- Enables effective detection and assessment of fraud risks through the design and application of analytics supported by reliable, complete, and well-prepared data.
- Supports timely, informed decision-making by clearly communicating relevant fraud insights to appropriate stakeholders.
- Drives prompt and sustainable resolution of identified fraud issues through effective remediation actions and structured follow-up processes.
- Sustains a strong and evolving fraud risk posture by delivering targeted, role-based training and regularly refreshing internal audit testing in response to emerging fraud risks.

Example Key Control Areas for Fraud Risk

- Accounts Payable and Disbursements
- Vendor and Third-Party Management
- Customer or Client Onboarding
- Identity and Access Management
- Monitoring and Detection Activities
- Financial Reporting and Accounting
- Sales, Contracting, and Revenue Recognition
- Payroll and Workforce Administration
- Inventory and Asset Management
- Expense Reimbursement and Procurement Cards
- Incident Management and Reporting Channels

4. 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 effective and trustworthy manner.
- 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.

Grant Thornton

Fraud Investigation and Corrective Action

Investigations serve multiple purposes: **to determine what happened**, **identify responsible parties**, **assess control breakdowns**, **inform remediation efforts**, and **prevent reoccurrence**.

Designing an End-to-End Investigations Process

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. Key design considerations include:

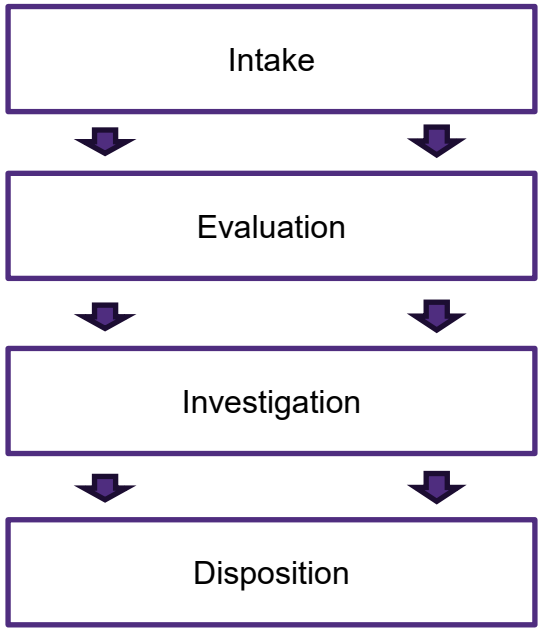
- Standardized intake and triage
- Clear roles and responsibilities
- Escalation criteria and decision points
- Engagement with legal

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

- Hold internal stakeholders accountable
- Remediate control deficiencies

Example Investigation Lifecycle



5. Fraud Risk Management Monitoring Activities

- The FRM program is not a “set it and forget it” exercise.
- Monitoring activities provide insight into performance, emerging issues, and whether corrective actions are closing the gaps they were designed to address.

Fraud Risk Management Monitoring Activities

The organization needs a disciplined approach to monitoring whether the FRM program is operating as intended and aligned to risk appetite.

FRM monitoring activities should answer three questions:

1. Is the program present and functioning?
2. Is it effective?
3. Is it improving over time?

To achieve this, organizations generally use a mix of:

- **Ongoing monitoring**—built into day-to-day activities
  - Management review of dashboards
  - Oversight of key initiatives
  - Key Risk Indicators (KRIs) to track changes in exposure in relation to risk appetite.
  - Key Performance Indicators (KPIs) to track how well the FRM program is functioning.

- **Separate evaluations**—periodic, more in-depth reviews
  - Internal audit independent assessments / testing
  - Third-party program assessments

Fraud Risk Management: Ongoing Monitoring Approaches

Reporting frequency should be **risk-based**.

Escalation triggers should be clearly defined so that issues are rapidly elevated outside the normal reporting cycle.

A strong monitoring framework translates the FRM strategy into a small, focused set of metrics.

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

- **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.

Role of Internal Audit

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

- The design and implementation of the Fraud Risk Management (FRM) program is effective;
- FRM governance is documented, consistently applied and understood;
- Fraud controls are well designed and operating effectively;
- FRM monitoring activities are well-designed, properly executed, and based on reliable data.
- Prior findings and recommendations have been addressed in a timely and sustainable manner.

By combining **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.

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.

Thank you!

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

Grant Thornton Advisors LLC and its subsidiary entities are not licensed CPA firms. For additional information on matters covered in this presentation, contact a Grant Thornton Advisors LLC professional.

This Grant Thornton Advisors LLC content provides information and comments on current issues and developments. It is not a comprehensive analysis of the subject matter covered. It is not, and should not be construed as, accounting, legal, tax, or professional advice provided by Grant Thornton Advisors LLC. All relevant facts and circumstances, including the pertinent authoritative literature, need to be considered to arrive at conclusions that comply with matters addressed in this content.

Grant Thornton Advisors LLC and its subsidiary entities are not licensed CPA firms.

For additional information on topics covered in this content, contact a Grant Thornton Advisors LLC professional.

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

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

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