



FRAUD RISK MANAGEMENT GUIDE

Second
Edition

EXECUTIVE SUMMARY

COSO

Committee of Sponsoring
Organizations of the
Treadway Coāmission

 **ACFE**
Association of Certified Fraud Examiners

Principal Authors of the *Fraud Risk Management Guide*

David L. Cotton, CPA, CFE, CGFM

Chairman Emeritus, Cotton, A Sikich Company

Sandra Johnigan, CPA/CFF, CFE

Owner, Johnigan, P.C.

Leslye Givarz

Technical Editor, Public Company Accounting Oversight Board (Retired)

Acknowledgements

COSO and ACFE thank each of the Fraud Risk Management Update Task Force members, the other anti-fraud professionals who provided recommendations for this *Fraud Risk Management Guide Update*, and the original Task Force and Advisory Panel members for their generous contributions of time, resources, and knowledge (see pages 5 to 7).

In particular, COSO and ACFE gratefully acknowledge David L. Cotton and Sandra K. Johnigan, co-chairs of the Fraud Risk Management Update Task Force, for their outstanding leadership and efforts toward the completion of this Guide.

COSO Board Members

Paul J. Sobel

Outgoing COSO Chair

Lucia Wind

Incoming COSO Chair

Douglas F. Prawitt

American Accounting Association

Jeffrey C. Thomson

Institute of Management Accountants (Outgoing Board Member)

Jennifer Burns

American Institute of CPAs

Larry R. White

Institute of Management Accountants (Incoming Board Member)

Daniel C. Murdock

Financial Executives International

Patty K. Miller

The Institute of Internal Auditors

Preface

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence.

COSO is a private-sector initiative jointly sponsored and funded by the following organizations:



American Accounting Association (AAA)



American Institute of CPAs (AICPA)



Financial Executives International (FEI)



The Institute of Management Accountants (IMA)



The Institute of Internal Auditors (IIA)

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org



FRAUD RISK MANAGEMENT GUIDE

Second
Edition

EXECUTIVE SUMMARY

March 2023 | Research Commissioned by

COSO

Committee of Sponsoring
Organizations of the
Treadway Coāmission

Co-published by

 **ACFE**
Association of Certified Fraud Examiners



FOREWORD

In 1992 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) released its *Internal Control — Integrated Framework* (the original framework). The original framework gained broad acceptance and was widely recognized as a leading framework for designing, implementing, and conducting internal control and assessing the effectiveness of internal control.

COSO revised the original framework in 2013 (COSO 2013 IC Framework). The COSO 2013 IC Framework incorporated 17 principles. These 17 principles are associated with the five internal control components, and provide clarity for the user in designing and implementing systems of internal control and for understanding requirements for effective internal control. COSO makes clear that for a system of internal control to be effective, each of the 17 principles is present, functioning, and operating together in an integrated manner. One important principle focused on fraud risk.

Principle 8, one of the risk assessment component principles, states:
The organization considers the potential for fraud in assessing risks to the achievement of objectives.

The *Fraud Risk Management Guide*, originally published in 2016, was intended to be supportive of and consistent with the COSO 2013 IC Framework and to serve as guidance for organizations to follow in addressing this specific fraud risk assessment principle.

Fraud is not static, however. Accordingly, COSO and ACFE initiated an update process that included reaching out to a broad range of users for recommendations on where the *Fraud Risk Management Guide* could be improved, and assembled a team to take a refreshed look at the Guide and assess how and where it should be updated.

Performing periodic fraud risk assessments is an important element of good governance. Additionally, it is also a COSO 2013 IC Framework requirement.

For organizations desiring a more comprehensive approach to managing fraud risk, the *Fraud Risk Management Guide* includes the information needed to perform a fraud risk assessment, as well as guidance on establishing an overall Fraud Risk Management Program including:

- Establishing fraud risk governance policies
- Performing a fraud risk assessment
- Designing and deploying fraud preventive and detective control activities
- Conducting investigations, and
- Monitoring and evaluating the total Fraud Risk Management Program

This Guide is designed to be familiar to COSO Framework users. It contains *principles* and *points of focus*. This Guide's five principles are consistent with the five COSO Internal Control Components and the 17 COSO principles.

This Guide updates the first edition of the *Fraud Risk Management Guide* published in 2016. It also draws from a 2008 publication published and sponsored by the American Institute of CPAs (AICPA), Institute of Internal Auditors (IIA), and Association of Certified Fraud Examiners (ACFE). This prior publication, *Managing the Business Risk of Fraud: A Practical Guide*, contained similar guidance for establishing a comprehensive Fraud Risk Management Program and has been used by many organizations to manage fraud risk. The COSO sponsors and ACFE are appreciative of the work done by the task forces that produced these prior publications. This updated Guide builds on them by addressing more recent anti-fraud developments, revising terminology to be consistent with newer COSO terminology, and adding important information related to technology developments — specifically data analytics.

The Guide's executive summary provides a high-level overview intended for the board of directors, senior management, and chief audit executives. It is designed to explain the benefits of establishing strong anti-fraud policies and controls. The updated Guide's appendices contain valuable information:

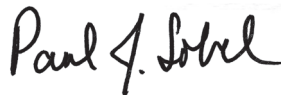
- A. Glossary
- B. Fraud Risk Management Roles and Responsibilities
- C. Fraud Risk Management Considerations for Smaller Entities
- D. Data Analytics and FRM
- E. Fraud Risk Assessment Example
- F. Fraud Risk Management Tools
- G. Managing the Risk of Fraud, Waste, and Abuse in the Government Environment

The updated Guide also contains links to several valuable tools and templates that can be used to make implementation and documentation of a comprehensive Fraud Risk Management Program more effective.

COSO has also published *Enterprise Risk Management — Integrating with Strategy and Performance* (COSO 2017 ERM Framework). This Guide, the COSO 2013 IC Framework, and the COSO 2017 ERM Framework, are intended to be complementary. Depending on how an organization implements the *Internal Control Framework*, the *ERM Framework*, and this Guide, there may be overlapping and interconnecting areas. Fraud risk can affect areas beyond accounting and financial management activities. Indeed, an organization seeking to minimize the adverse impacts of fraud needs to consider fraud risk in all areas of the enterprise and its operations.

The COSO Board would like to thank members of the Task Force that updated this Guide, the other anti-fraud professionals who provided recommendations for this Update, the original Task Force and Advisory Panel members, and the COSO member organizations for their contributions in reviewing the Guide (see pages 5, 6, and 7).

Finally, the COSO Board gratefully acknowledges David L. Cotton and Sandra K. Johnigan, co-chairs of the Update Task Force, for their outstanding leadership and efforts toward the completion of this update.



Paul J. Sobel
COSO Chair



Bruce Dorris
ACFE President and CEO

Fraud Risk Management Guide Update Task Force

Tom Caulfield
Procurement Integrity Consulting Services

Sandra K. Johnigan, Co-Chair
Johnigan, PC

Jeffrey Steinhoff
Formerly KPMG and GAO

David Coderre
CAATS

Andi McNeal
ACFE

Pamela Verick
Protiviti

David L. Cotton, Co-Chair
Cotton, A Sikich Company

Linda Miller
Audient Group, LLC

Vincent Walden
KonaAI

John D. Gill
ACFE

Lynda Schwartz
University of Massachusetts Amherst

Anti-Fraud Professionals Who Provided Recommendations for this Fraud Risk Management Guide Update

Tim Berichon
Institute of Internal Auditors

Anne Mercer
Institute of Internal Auditors

Sonia Boguslavsky
Bank of Israel

Rhod Newcombe
Brit Insurance

Dr. El-fred Boo
Nanyang Technological University

Joseph Palmar
Palmar Forensics

Mike Carter
Bittrex, Inc.

Brad Preber
Grant Thornton

Margot Cella
Center for Audit Quality

Katherine Robinson
Sterling Bank & Trust, FSB

Dr. Todd DeZoort
The University of Alabama

Valerie Scarantino
UGI Corporation

Scott Hilsen
Cox Automotive, Inc.

Paul Sobel
COSO Chairman

Robert Hirth
Protiviti

Dr. Robert Tennant
Institute of Management Accountants

Robert Hogan
Hogan Forensics

Lucy Wang
Center for Audit Quality

Ryan Hubbs
Schlumberger

Elizabeth Zachem Woodward
Dean Dorton

Jonathan T. Marks
Baker Tilly US, LLP

In addition to the Task Force and Anti-Fraud Professionals listed above who contributed to the development of this 2023 Update, COSO and ACFE gratefully acknowledge those listed below, who previously contributed to the 2016 Guide.

Fraud Risk Management Task Force

Barbara Andrews
AICPA

Dan George
USAC

Kelly Richmond Pope
DePaul University

Michael Birdsall
Comcast Corporation

John D. Gill
ACFE

Carolyn Devine Saint
University of Virginia

Toby Bishop
Formerly ACFE, Deloitte

Leslye Givarz
Formerly AICPA, PCAOB

Jeffrey Steinhoff
Formerly KPMG and GAO

Margot Cella
Center for Audit Quality

Cindi Hook
Comcast Corporation

William Titera
Formerly EY

David Coderre
CAATS

Sandra K. Johnigan, Co-Chair
Johnigan, PC

Michael Ueltzen
Ueltzen & Company

David L. Cotton, Chair
Cotton, A Sikich Company

Bill Leone
Norton Rose Fulbright

Pamela Verick
Protiviti

James Dalkin
GAO

Andi McNeal
ACFE

Vincent Walden
KonaAI

Ron Durkin
Durkin Forensic, Inc.

Linda Miller
Audient Group, LLC

Bill Warren
PwC

Bert Edwards
Formerly State Department

Kemi Olateju
General Electric

Richard Woodford
U.S. Coast Guard Investigative Service

Frank Faist
Charter Communications

Chris Pembroke
Crawford & Associates, PC

Eric Feldman
Affiliated Monitors, Inc.

J. Michael Peppers
University of Texas

Fraud Risk Management Advisory Panel

Dan Amiram

Columbia University Business School

Zahn Bozanic

The Ohio State University

Greg Brush

Tennessee Comptroller of Treasury

Tamia Buckingham

Massachusetts School Building Authority

Ashley L. Comer

James Madison University

Molly Dawson

Cotton & Company LLP

Eric Eisenstein

Cotton & Company LLP

Michael Justus

University of Nebraska

Theresa Nellis-Matson

New York Office of the State Comptroller

Jennifer Paperman

New York Office of the State Comptroller

Daniel Rossi

New York Office of the State Comptroller

Lynda Harbold Schwartz

University of Massachusetts Amherst

Rosie Tomforde

Regional Government

The COSO Board gratefully acknowledges everyone who contributed their time, experience, thoughts, and expertise to both the original Guide and this updated Guide.



EXECUTIVE SUMMARY | FRAUD RISK MANAGEMENT

The Ever-Present Risk of Fraud and its Costs

All organizations are subject to fraud risks. Some organizational leaders may question whether the benefits derived from implementing and maintaining a Fraud Risk Management Program outweigh the costs. This Guide demonstrates why the answer to that question is Yes, and provides help in implementing such a program.

Publicized fraudulent behavior by key executives, other employees, and outsiders repeatedly demonstrate the reality of this ever-present risk and how it negatively impacts reputations, brands, and images of many organizations around the globe. Large frauds have led to the collapse of entire organizations, massive asset losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets, government, and not-for-profit entities. Even relatively small frauds can be devastating to an organization, resulting in:

- Loss of trust in management and the breakdown of teamwork and organizational cohesion
- Increased scrutiny from law enforcement and regulatory bodies
- Loss of trust by stakeholders (shareholders, donors, customers, taxpayers, and the public)
- Increased employee and management turnover
- Reputational damage
- Loss of competitive advantage

It is impossible and impractical to eliminate all fraud in all organizations. However, effective leaders address fraud risk as they do any risk — they manage it. The *Fraud Risk Management Guide* provides a blueprint to do just that. It is based on the proven principles of enterprise risk management as published by COSO, most recently in 2017. This Guide gives organizations, whether large or small, government or private, profit or non-profit, the information necessary to design a plan specific to the risks for that entity. There is no “one size fits all approach” to managing fraud risk. But with the right approach, an organization can create a custom-fitted program tailored to its specific needs.

A Growing Area of Fraud Risk

Organizations committed to fraud prevention, detection, and deterrence will address not just *internal* fraud risks — frauds perpetrated by parties within the organization, but also *external* fraud risks — fraud perpetrated on the organization by outside parties such as ransomware, data breaches, identity theft, and a wide range of corruption schemes that continue to evolve.

Fraud Deterrence Now and in the Future

Implementation of the principles in this Guide will maximize the likelihood that fraud will be prevented or detected in a timely manner and can create a strong fraud deterrence effect.

COSO’s mission is *to help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence*. The *Fraud Risk Management Guide* is a key tool for furthering this mission, particularly with respect to fraud deterrence.

As a first step in discussing fraud deterrence, the following practical definition of fraud¹ is used in this Guide:

Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

Therefore, to successfully achieve fraud deterrence, organizations will implement policies and procedures that target the prevention and detection of fraud. Organizations that implement a rigorous Fraud Risk Management Program will further strengthen fraud deterrence by making it known that potential fraud perpetrators face a significant likelihood of getting caught and being punished.

Deterrence is also supported and enhanced by the knowledge throughout the organization that:

- Those charged with governance have made a commitment to comprehensive fraud risk management

¹ The authors recognize that many other definitions of fraud exist, including those developed by the Auditing Standards Board of the American Institute of Certified Public Accountants, the Public Company Accounting Oversight Board, and the Government Accountability Office. Some legal definitions of fraud do not include scienter, or intent.

- Periodic fraud risk assessments are being conducted and updated as risks change or new information becomes known
- Fraud preventive and detective control activities, including data analytics — overt and covert — are being conducted
- Suspected frauds are investigated quickly
- Fraud reporting mechanisms are in place
- Discovered frauds are remediated thoroughly
- Wrongdoing has been appropriately disciplined
- The entire Fraud Risk Management Program is being constantly monitored

Roles and Responsibilities

The board of directors² and top management have responsibility for managing fraud risk. In particular, they are expected to understand how the organization is responding to heightened risks and emerging exposures, as well as public and stakeholder scrutiny; what form of Fraud Risk Management Program the organization has in place; how it identifies fraud risks; what it is doing to better prevent fraud, or at least detect it sooner; and what processes are in place to investigate fraud and take corrective action. Further, personnel at all levels of the organization have a responsibility to understand the effects of fraud and the importance of preventing fraud. This Guide is designed to help address these complex issues.

How it Works

This Guide provides implementation guidance for a Fraud Risk Management Program that defines principles and points of focus for fraud risk management and describes how organizations of various sizes and types can establish their own Fraud Risk Management Programs. The Guide includes examples of key program components and resources that organizations can use as a starting place to develop a Fraud Risk Management Program effectively and efficiently. In addition, and recognizing that no two organizations are the same, the Guide contains references to other sources of guidance to allow for tailoring a Fraud Risk Management Program to a particular industry or to government or not-for-profit organizations. Each organization will assess the degree of emphasis to place on fraud risk management based on its size and circumstances.

The Guide also contains valuable information for users who are implementing a Fraud Risk Management Program. This includes addressing fraud risk management roles and responsibilities, fraud risk management considerations for smaller organizations, data analytics, and managing fraud risk in the government environment.

What's New in the 2022 *Fraud Risk Management Guide*

Following publication of the *Fraud Risk Management Guide* in 2016, it became recognized as containing a widely accepted set of leading practices for anti-fraud professionals and organizations intent on deterring fraud. But, fraud is not static. Accordingly, COSO and ACFE initiated an update process that included reaching out to a broad range of users for recommendations on where the Guide can be improved, and assembled a team to take a refreshed look at the Guide and assess how and where it should be updated. Following are the key changes to this 2022 edition:

- **Fraud risk management and deterrence.** This edition explains how fraud risk management relates to and supports fraud deterrence — a key theme in COSO's missions.
- **Relationships among COSO's two frameworks and fraud risk management.** This edition explains how the COSO 2013 *Internal Control — Integrated Framework*, the COSO 2017 *Enterprise Risk Management — Integrating with Strategy and Performance Framework* and the *Fraud Risk Management Guide* are related and support each other.
- **Expanded information on data analytics.** Data analytics continues to grow in importance as a key tool for the prevention and early detection of fraud. Advanced applications of data analytics may be less familiar to some users than standard tools, such as interviewing and whistleblower systems. Accordingly, this edition includes expanded and updated information on data analytics, while continuing to emphasize the importance of interviewing and whistleblower systems. A data analytics Point of Focus has been added to each of the five fraud risk management principles to demonstrate how the use of data analytics is an integral part of each principle. Further, the data analytics appendix has been updated and expanded. This approach is not meant to downplay the importance of other tools, but rather, to highlight the increasing power of data analytics in managing fraud risk.

² Throughout this Guide the terms *board* and *board of directors* refer to the governing or oversight body or those charged with governance of the organization. The terms *chief executive officer* (CEO) and *chief financial officer* (CFO) refer to the senior-level management individuals responsible for overall organization performance and financial reporting.

- **Internal control and fraud risk management.** This edition explains how **internal control** and fraud risk management are related and support each other, but are different in some important respects. Examples are provided to show that many “go-to” internal control processes and procedures may be adequate for ensuring accuracy in accounting and financial reporting but may not provide sufficient fraud protection.
- **Assessing the effectiveness of existing control procedures as related to fraud risk.** Chapter 2 (Fraud Risk Assessment) provides additional information on this important step in the fraud risk assessment process. It clarifies and emphasizes that assessing control effectiveness involves (a) identifying existing control procedures related to each identified inherent fraud risk, (b) assuring that the controls have been implemented and are working as designed, and (c) assessing whether the controls are adequate to address the fraud risks that have been identified. That last step is in addition to an assessment of the design and operating effectiveness of controls from an internal control over financial reporting perspective. Further, it is the key to identifying residual fraud risk so that additional fraud control activities such as additional data analytics can be applied.
- **Changes in the legal and regulatory environment.** This edition includes updated information with respect to recent legal and regulatory developments in the U.S. pertaining to fraud and fraud risk management, including:
 - The Department of Justice’s *Evaluation of Corporate Compliance Programs*
 - The Government Accountability Office’s *A Framework for Managing Fraud Risks in Federal Programs*
 - U.S. Securities and Exchange Commission’s Climate and Environmental, Social, and Governance (ESG) Task Force Reports
- **Fraud reporting systems or hotlines.** ACFE research consistently shows that the majority of frauds are discovered through tips, often from employees in an organization. This edition includes updated and expanded information related to the importance of fraud reporting systems in detecting, preventing, and deterring fraud.
- **Changes in the external environment and fraud landscape.** The fraud landscape is changing rapidly. This edition includes information on this changing environment, including:
 - Environmental, Social, and Governance (ESG) initiatives and reporting
 - Cyber fraud
 - Blockchain, cryptocurrency, and digital assets
 - Ransomware
 - COVID-19 response efforts, the CARES Act (Public Law 116-136) and other related programs
 - Remote working and hybrid working environments
 - Innovative and virtual management tools and accounting procedures
- **Appendices changes.** The 2016 Guide had 19 appendices. This 2022 edition has 7. Several of the 2016 appendices have been moved to ACFE’s [Fraud Risk Management Tools](#) web site so that they can be updated as needed. The appendices moved are:
 - Sample Fraud Control Policy Framework (2016 Appendix F-1)
 - Fraud Risk Management High-Level Assessment (2016 Appendix F-2)
 - Sample Fraud Policy Responsibility Matrix (2016 Appendix F-3)
 - Sample Fraud Risk Management Policy (2016 Appendix F-4)
 - Sample Fraud Risk Management Survey (2016 Appendix F-5)
 - Fraud Risk Exposures (2016 Appendix G)
 - The five Fraud Risk Management Scorecards (2016 Appendices I-1 through I-5)

The Appendix, Managing the Risk of Fraud, Waste, and Abuse in the Government Environment, has been updated and expanded, and remains in the Guide as a valuable resource.

Finally, and significantly, the ACFE tools site includes a greatly-expanded list of fraud risk exposures and fraud schemes. Each scheme in the expanded list is hyperlinked to an underlying description of the scheme and how it is carried out. This list contains generic schemes — schemes that can victimize any organization — but also industry-specific schemes (healthcare, financial services, manufacturing, and so forth). Again, through input from users, this resource will continue to expand. These dynamic resources are readily accessible to anti-fraud professionals implementing Fraud Risk Management Programs.

COSO and ACFE are confident that this updated *Fraud Risk Management Guide* will continue to grow in importance as the set of leading practices for preventing, detecting, and deterring fraud.

Fraud Risk Management and the COSO Internal Control Framework

COSO revised its *Internal Control — Integrated Framework* in 2013 to incorporate 17 principles. These 17 principles are associated with the five internal control components COSO established in 1992. The principles provide clarity for the user in designing and implementing systems of internal control and for understanding requirements for effective internal control. COSO clarifies that for a system of internal control to be effective, each of the 17 principles is present, functioning, and operating in an integrated manner. Throughout this Guide the COSO 2013 IC Framework has been used as a source for describing aspects of internal control.

Principle 8, one of the risk assessment component principles, states:
The organization considers the potential for fraud in assessing risks to the achievement of objectives.

This Guide is intended to be supportive of and consistent with the COSO 2013 IC Framework and can serve as guidance for organizations to follow in performing a fraud risk assessment.

For organizations desiring to establish a more comprehensive approach to managing fraud risk, however, this Guide includes more than just the information needed to perform a fraud risk assessment. It also provides guidance on establishing the other components of an overall Fraud Risk Management Program, including:

- Establishing fraud risk governance policies
- Designing and deploying fraud preventive and detective control activities
- Conducting investigations and taking corrective actions
- Monitoring and evaluating the total Fraud Risk Management Program

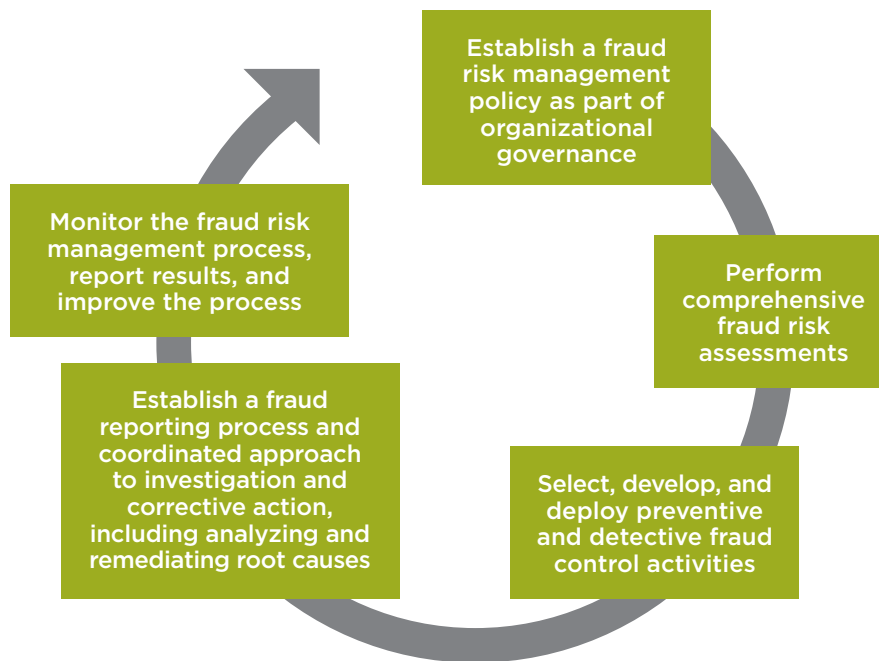
The Guide also defines important terminology (see Appendix A), explains key roles and responsibilities (see Appendix B), and describes how it can be applied to smaller organizations (see Appendix C).

Consequently, organizations applying the COSO 2013 IC Framework can choose from the following two approaches in addressing this important fraud risk assessment principle:

- **First Approach:** They can use this Guide's second fraud risk management principle (*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*) on a stand-alone basis to conduct a fraud risk assessment that is compliant with COSO 2013 IC Framework Principle 8. Under this approach, an organization would overlay this fraud risk assessment process on its existing internal control structure by revisiting each component of internal control and assessing vulnerabilities to fraud.
- **Second Approach:** They can implement this Guide as a separate, compatible, and more comprehensive process to not only periodically assess, but to also manage the organization's fraud risks as part of a broader Fraud Risk Management Program. That approach includes a fraud risk assessment and also encompasses fraud risk governance, designing and implementing fraud control activities, fraud investigation and corrective action, and fraud risk management evaluation and monitoring. Once the Guide is implemented, its results will support and will be consistent with the overall COSO 2013 IC Framework.

The second approach results in an ongoing, comprehensive Fraud Risk Management Program as follows in **Figure 1**.

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process



This comprehensive approach recognizes and emphasizes the fundamental difference between internal control weaknesses resulting in **errors** and weaknesses resulting in **fraud**. This fundamental difference is **intent**. An organization that simply adds the fraud risk assessment to the existing risk assessment may not thoroughly examine and identify possibilities for improper acts designed to:

- Misstate financial information
- Misstate non-financial information
- Misappropriate assets
- Perpetrate illegal acts or corruption

Implementing a specific and more focused *fraud* risk assessment as a separate Fraud Risk Management Program enhances the likelihood that the assessment's focus remains on intentional acts.

The recommended approach is also likely to result in a more robust and comprehensive assessment of fraud risk. It also provides the additional structure needed for comprehensive fraud risk management. If organizations use the more simplified approach (just performing the fraud risk assessment), they can combine those results with the COSO 2013 IC Framework's results to yield more robust prevention and detection mechanisms.

Relationships Among COSO's Two Frameworks and this *Fraud Risk Management Guide*

COSO published *Internal Control — Integrated Framework* in 2013 (COSO 2013 IC Framework) and published *Enterprise Risk Management — Integrating with Strategy and Performance* in 2017 (COSO 2017 ERM Framework). This *Fraud Risk Management Guide*, the COSO 2013 IC Framework, and the COSO 2017 ERM Framework, are intended to be complementary.

Depending on how an organization implements the *Internal Control Framework*, the ERM Framework, and this Guide, there may be overlapping and interconnecting areas. Fraud risk can affect all areas of accounting functions, financial management and reporting activities, and non-financial management and reporting activities. Indeed, an organization seeking to minimize the adverse impacts of fraud will consider fraud risk in all areas of the enterprise and its operations.

Enterprise risk management is broader than internal control in that it focuses on a variety of risk responses to manage risk in all aspects of business. Internal control is a subset and integral part of enterprise risk management, while enterprise risk management is a subset of organizational governance. Of course, fraud risk can impact all aspects of both enterprise risk and internal control.

This *Fraud Risk Management Guide* is intended to be an important component of a holistic risk response that is both effective and efficient in addressing wide-ranging fraud risks, including those originating from internal sources (e.g., management, employees, consultants), external sources (e.g., cyber/hacking risk), or both (e.g., conspiracy, corruption, money laundering, drug trafficking/terrorism financing).

Summary of Fraud Risk Management Components and Principles

Fraud Risk Governance

Fraud risk governance is an integral component of corporate governance and the internal control environment. Corporate governance addresses the manner in which the board of directors and management meet their respective obligations to achieve the organization's goals, including its fiduciary,

reporting, and legal responsibilities to stakeholders. The internal control environment creates the discipline that supports the assessment of risks to the achievement of the organization's goals.



Control Environment

Principle 1

The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.

Fraud Risk Assessments

A fraud risk assessment is a dynamic and iterative process for identifying and assessing fraud risks relevant to the organization. Fraud risk assessment addresses the risk of fraudulent financial reporting, fraudulent non-financial reporting, asset misappropriation, and corruption (including illegal acts and noncompliance with laws and regulations).

Organizations can tailor this approach to meet their individual needs, complexities, and goals. Fraud risk assessment is not only an integral component of risk assessment and internal control, it also is specifically linked to COSO 2013 IC Framework Principle 8.



Risk Assessment

Principle 2

The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

Fraud Control Activity

A fraud control activity is an action established through policies and procedures that helps ensure that management's directives to mitigate fraud risks are carried out. A fraud control activity is a specific procedure or process intended either to prevent fraud from occurring or to detect fraud quickly in the event that it occurs.

Fraud control activities are generally classified as either preventive (designed to avoid a fraudulent event or transaction at the time of initial occurrence) or detective (designed to discover a fraudulent event or transaction

after the initial processing has occurred). The selection, development, implementation, and monitoring of fraud preventive and fraud detective control activities are crucial elements of managing fraud risk. Fraud control activities are documented with descriptions of the identified fraud risk and scheme, the fraud control activity that is designed to mitigate the fraud risk, and the identification of those responsible for the fraud control activity. Fraud control activities are integral to the ongoing fraud risk assessment component of internal control.



Principle 3 The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.

Fraud Investigation and Corrective Action

Control activities cannot provide absolute assurance against fraud. As a result, the organization's governing board ensures that the organization develops and implements a system for prompt, competent, and confidential review, investigation, and resolution of instances of

allegations involving potential fraud and misconduct. An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation, by establishing and carefully preplanning investigation and corrective action processes.



Principle 4 The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

Fraud Risk Management Monitoring Activities

The fifth fraud risk management principle relates to monitoring the overall Fraud Risk Management Program. Organizations use fraud risk management monitoring activities to ensure that each of the five principles of fraud risk management is present and functioning as designed and that the organization identifies needed changes in a timely manner.

Organizations use ongoing and separate (periodic) evaluations, or some combination of the two, to perform

the fraud monitoring activities. Similar to the COSO 2013 IC Framework, ongoing evaluations in a Fraud Risk Management Program that are built into the organization's business processes at varying levels provide timely information. In contrast, organizations conduct separate evaluations periodically that vary in scope and timing based on numerous factors, including the results of ongoing evaluations.



Principle 5 The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

Use by Interested Parties

Board of Directors and Audit Committee

A well-performing and engaged board discusses with senior management the state of the entity's Fraud Risk Management Program and provides oversight as needed. Senior management has overall responsibility for the design and implementation of a Fraud Risk Management Program, including setting the tone at the top that creates the culture for the entire organization. The board establishes policies and procedures explaining how the board provides oversight, including defining expectations about integrity and ethical values, transparency, and accountability for the implementation and operation of the Fraud Risk Management Program. Senior management informs the board of the residual risks of fraud from its fraud risk assessments, as well as incidents of fraud or suspected fraud. The board challenges management and asks the tough questions, as necessary. It seeks input from internal auditors, external independent auditors, specialists, and legal counsel and utilizes these resources as needed to investigate any issues.

The board is an important check on the risk of management wrongdoing, including management override of anti-fraud and other internal controls. The board assesses the risk of management override and also considers and addresses fraud allegations related to senior management if they arise.

Senior Management

Senior management assesses the entity's Fraud Risk Management Program in relation to this *Fraud Risk Management Guide*, focusing on how the organization applies the five principles in support of its Fraud Risk Management Program. Further, they assess the entity's fraud risk in compliance with Principle 8 of the COSO 2013 IC Framework.

Other Management and Personnel

Managers and other personnel consider how they are conducting their responsibilities in light of this Guide and discuss with more senior personnel ideas for strengthening fraud risk controls. More specifically, they consider how existing controls affect the relevant principles within the five components of fraud risk management, as well as Principle 8 of the COSO 2013 IC Framework.

Internal Audit

Internal auditors review their internal audit plans and how the plans are applied to the entity's Fraud Risk Management Program in connection with implementation of this guidance. Internal auditors will use this Guide to 1) assess how effective their risk assessments are in evaluating fraud risk and improve them, and 2) help assess fraud risk in each internal audit project, and 3) identify potential control enhancements to minimize ongoing fraud risk.

External Independent Auditors

In many situations, an external independent auditor is engaged to audit or examine the effectiveness of the client's internal control over financial reporting in addition to auditing the entity's financial statements. The COSO 2013 IC Framework introduced Principle 8: the organization considers the potential for fraud in assessing risks to the achievement of objectives. Auditors can assess the entity's implementation of that Principle using this Guide.

Specialists

In addition to the audit committee, internal audit, and management, the organization also may include internal and external professionals with specific domain expertise, such as legal, compliance, investigations, emerging markets, human resources, security, and data analytics.

Other Professional Organizations

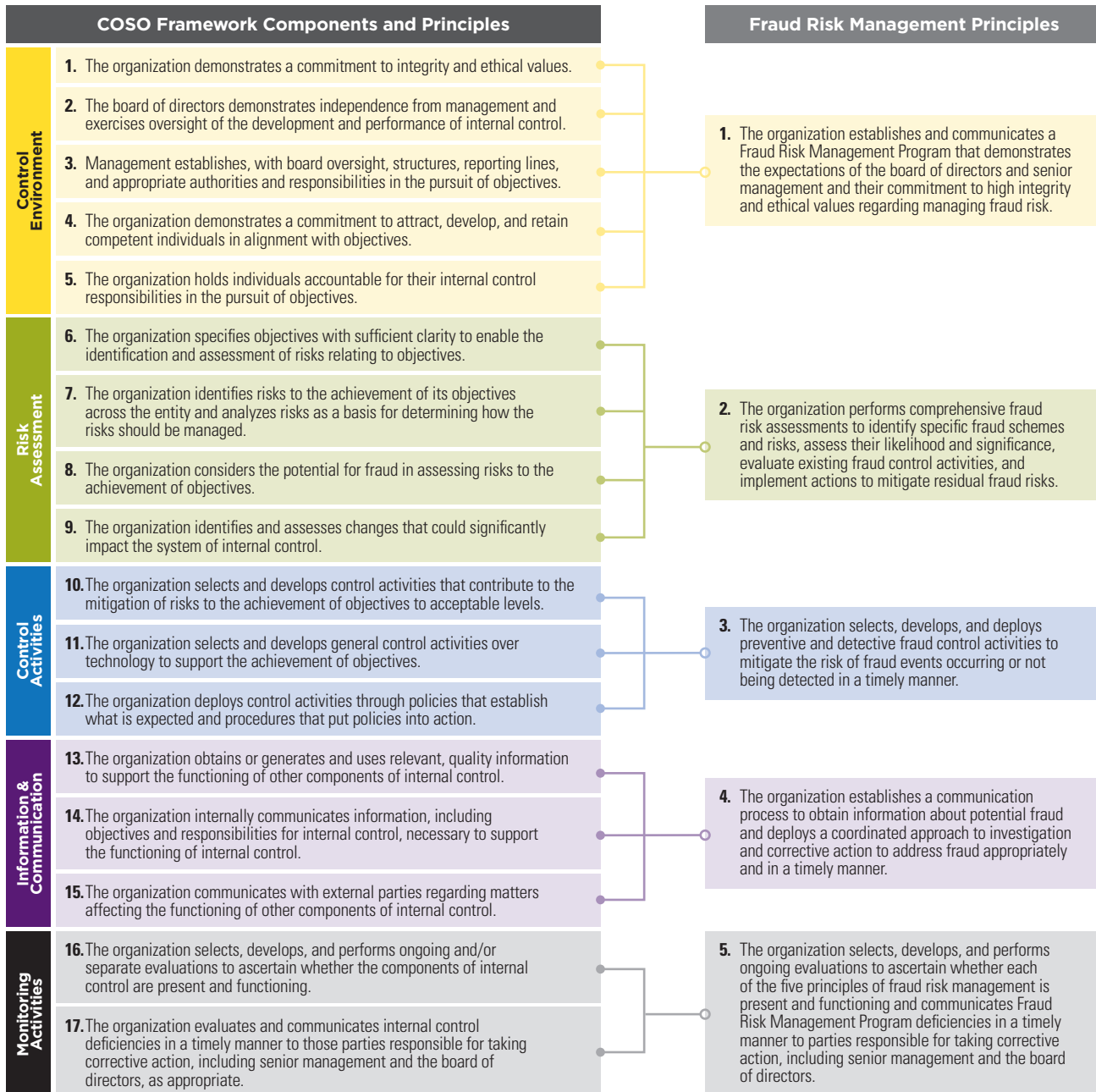
Other professional organizations providing guidance on fraud risk as it relates to operations, reporting, and compliance may consider their standards and guidance in comparison to the Guide. To the extent diversity in concepts and terminology is eliminated, all parties benefit.

Educators

The concepts of fraud risk management are important to professional education. Because fraud risks are pervasive and perennial, every professional benefits from a solid grounding in the Guide's concepts and approaches. Educators can leverage the Guide as a teaching text or as source material for lessons in leadership, business decision-making, management and organizational behavior, ethics, advanced audit, information management, data analytics, and forensic accounting.

Relationship Between the COSO 2013 IC Framework's Five Components and 17 Internal Control Principles and this Guide's Five Fraud Risk Management Principles

COSO revised its *Internal Control — Integrated Framework* in 2013 to incorporate 17 principles. These 17 principles are associated with the five internal control components COSO established in 1992. This Guide's five fraud risk management principles fully support, are entirely consistent with, and parallel the COSO 2013 IC Framework's 17 internal control principles. The correlation between the fraud risk management principles and the COSO 2013 IC Framework's internal control components and principles is as follows:



The most obvious correlation between these two sets of principles is COSO 2013 IC Framework Principle 8 and Fraud Risk Management Principle 2. In addition, as the above exhibit displays, all of the COSO 2013 IC Framework and Fraud Risk Management Principles correlate with and support each other.

FRAUD RISK MANAGEMENT GUIDE Second Edition

EXECUTIVE SUMMARY



Committee of Sponsoring
Organizations of the
Treadway Commission





FRAUD RISK MANAGEMENT GUIDE

Second
Edition

COSO

Committee of Sponsoring
Organizations of the
Treadway Commission

 **ACFE**
Association of Certified Fraud Examiners