

Fraud

Risk Management Guide

EXECUTIVE SUMMARY



Committee of Sponsoring
Organizations of the
Treadway Commission

Principal Authors

David L. Cotton, CPA, CFE, CGFM
Chairman, Cotton & Company LLP

Sandra Johnigan, CPA/CFF, CFE
Owner, Johnigan, P.C.

Leslye Givarz, CPA
Technical Editor, Public Company Accounting Oversight Board (Retired)

Acknowledgements

COSO and ACFE thank each of the Fraud Risk Management Task Force and Advisory Panel members (see Page vii) for their generous contributions of time, resources and knowledge.

In particular, COSO and ACFE gratefully acknowledge David L. Cotton, Chair of the Fraud Risk Management Task Force, for his outstanding leadership and efforts toward the completion of this guide.

COSO Board Members

Robert B. Hirth, Jr.
COSO Chair

Mitchell A. Danaher, CMA
Financial Executives International

Douglas F. Prawitt, Ph.D., CPA
American Accounting Association

Sandra Richtermeyer, Ph.D., CMA, CPA
Institute of Management Accountants

Charles Landes, CPA
American Institute of CPAs (AICPA)

Richard F. Chambers, CIA, QIAL, CGAP, CCSA, CRMA
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 providing thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control, and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations. COSO is a private-sector initiative jointly sponsored and funded by the following organizations:



American Accounting Association (AAA)
aaahq.org



The Institute of Management Accountants (IMA)
imanet.org



American Institute of CPAs (AICPA)
aicpa.org



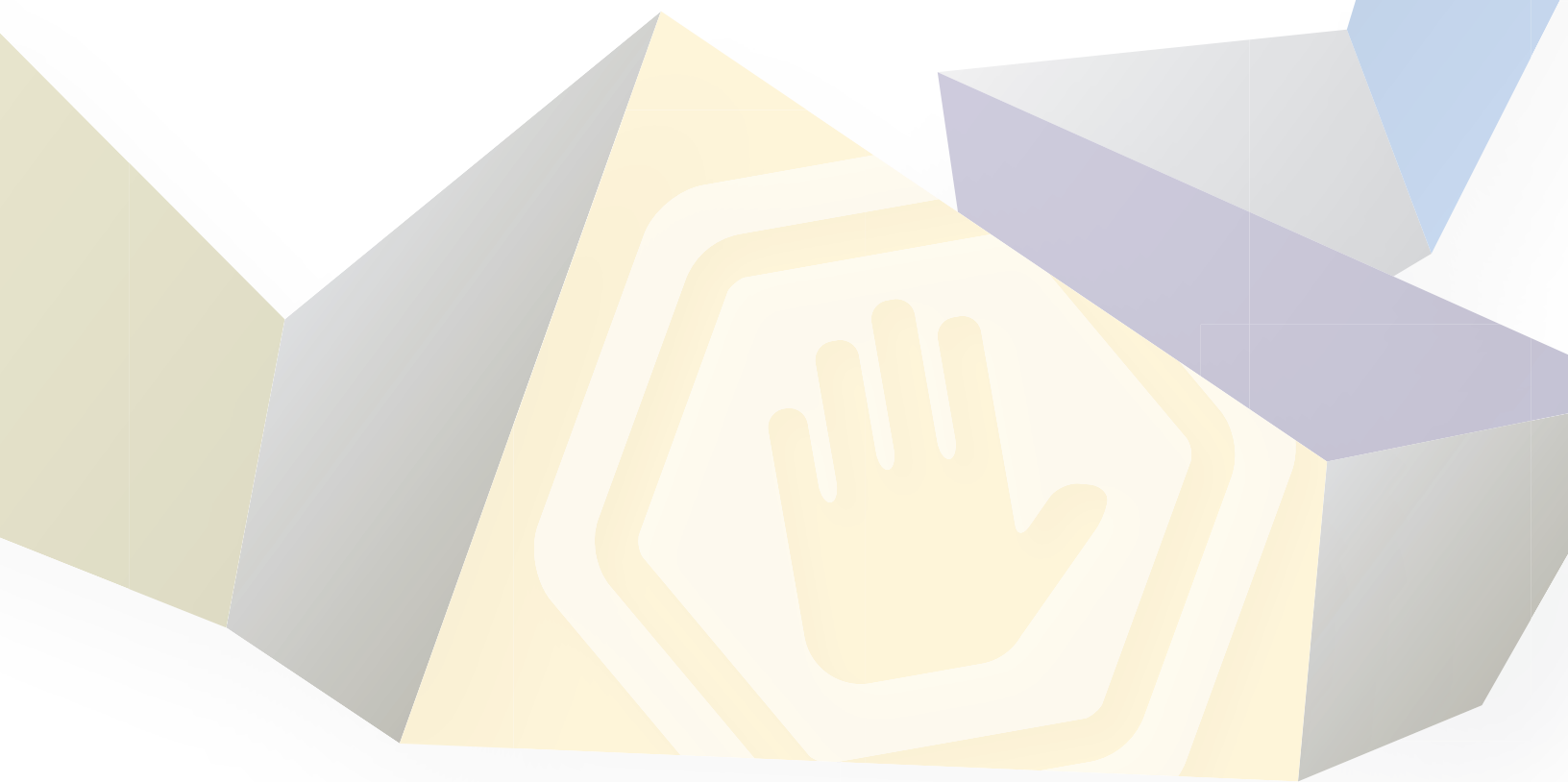
The Institute of Internal Auditors (IIA)
theiia.org

Financial Executives International (FEI)
financialexecutives.org

Fraud

Risk Management Guide

EXECUTIVE SUMMARY



September, 2016

Research Commissioned by



Committee of Sponsoring
Organizations of the
Treadway Commission

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 has gained broad acceptance and is widely used around the world. It is 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 (2013 framework). The 2013 framework incorporates 17 principles.¹ 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.

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 publication, *Fraud Risk Management Guide* (guide), is intended to be supportive of and consistent with the 2013 Framework and can serve as best practices guidance for organizations to follow in addressing this new fraud risk assessment principle.

For organizations desiring to establish a more comprehensive approach to managing fraud risk, this guide includes more than just the information needed to perform a fraud risk assessment. It also includes 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*.² This guide's five principles are consistent with the five COSO Internal Control Components³ and the 17 COSO principles.

This guide draws from and updates a 2008 product 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. COSO is appreciative of the work done by the task force that produced this prior publication. This new guide builds on that previous product by updating it for more recent developments, revising terminology to be consistent with newer COSO terminology, and adding important information related to technology developments — specifically data analytics.

¹ Per the 2013 COSO Framework, relevant principles "represent fundamental concepts associated with components" of internal control.

² Per the 2013 COSO Framework, points of focus are "important characteristics of principles."

³ Per the 2013 COSO Framework, a component is "one of five elements of internal control. The internal control components are the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring Activities."

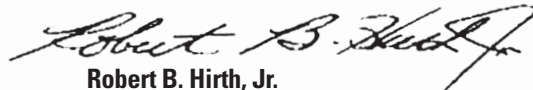
The guide's executive summary provides a high-level overview intended for the board of directors and senior management and is designed to explain the benefits of establishing strong anti-fraud policies and controls. The guide's appendices contain valuable templates, samples, examples, and tools to assist users in implementing the guide's best practices.

In addition, the guide contains hyperlinks to several valuable automated 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 — Integrated Framework (ERM Framework)*. This guide, the 2013 COSO Framework, and the 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 developed this guide, the Advisory Panel that reviewed drafts of the guide and provided valuable feedback, and the COSO Advisory Council for their contributions in reviewing the guide.

Finally, the COSO Board gratefully acknowledges David L. Cotton, Chair of the Task Force, for his outstanding leadership and efforts toward the completion of this guide.



Robert B. Hirth, Jr.
COSO Chair



James D. Ratley
ACFE President and CEO

Fraud Risk Management Task Force

Barbara Andrews
AICPA

Bert Edwards
Formerly State Department

Bill Leone
Norton Rose Fulbright

Jeffrey Steinhoff
KPMG

Michael Birdsall
Comcast Corporation

Frank Faist
Charter Communications

Andi McNeal
ACFE

William Titera
Formerly EY

Toby Bishop
Formerly ACFE, Deloitte

Eric Feldman
Affiliated Monitors, Inc.

Linda Miller
GAO

Michael Ueltzen
Ueltzen & Company

Margot Cella
Center for Audit Quality

Dan George
USAC

Kemi Olateju
General Electric

Pamela Verick
Protiviti

David Coderre
CAATS

John D. Gill
ACFE

Chris Pembroke
Crawford & Associates, PC

Vincent Walden
EY

David L. Cotton, Chair
Cotton & Company LLP

Leslye Givarz
Formerly AICPA, PCAOB

J. Michael Peppers
University of Texas

Bill Warren
PwC

James Dalkin
GAO

Cindi Hook
Comcast Corporation

Kelly Richmond Pope
DePaul University

Richard Woodford
U.S. Coast Guard
Investigative Service

Ron Durkin
Durkin Forensic, Inc.

Sandra K. Johnigan
Johnigan, PC

Carolyn Devine Saint
University of Virginia

Fraud Risk Management Advisory Panel

Dan Amiram
Columbia University Business School

Michael Justus
University of Nebraska

Zahn Bozanic
The Ohio State University

Theresa Nellis-Matson
New York Office of the State Comptroller

Greg Brush
Tennessee Comptroller of Treasury

Jennifer Paperman
New York Office of the State Comptroller

Tamia Buckingham
Massachusetts School Building Authority

Daniel Rossi
New York Office of the State Comptroller

Ashley L. Comer
James Madison University

Lynda Harbold Schwartz
Upland Advisory LLC

Molly Dawson
Cotton & Company LLP

Rosie Tomforde
Regional Government

Eric Eisenstein
Cotton & Company LLP

The COSO Board gratefully acknowledges David L. Cotton, Chair of the Fraud Risk Management Task Force, for his outstanding leadership and efforts toward the completion of this guide.

Executive Summary | Fraud Risk Management

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.⁴

All organizations are subject to fraud risks. It is impossible to eliminate all fraud in all organizations. However, implementation of the principles in this guide will maximize the likelihood that fraud will be prevented or detected in a timely manner and will create a strong fraud deterrence effect.

The board of directors⁵ and top management and personnel at all levels of the organization — including every level of management, staff, and internal auditors — have responsibility for managing fraud risk. Particularly, they are expected to understand how the organization is responding to heightened risks and regulations, 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 process is in place to investigate fraud and take corrective action. This *Fraud Risk Management Guide* (guide) is designed to help address these complex issues.

This guide recommends ways in which governing boards, senior management, staff at all levels, and internal auditors can deter fraud in their organization. Fraud deterrence is a process of eliminating factors that may cause fraud to occur. Deterrence is achieved when an organization implements a fraud risk management process that:

- Establishes a visible and rigorous fraud governance process
- Creates a transparent and sound anti-fraud culture

- Includes a thorough fraud risk assessment periodically
- Designs, implements, and maintains preventive and detective fraud control processes and procedures
- Takes swift action in response to allegations of fraud, including, where appropriate, actions against those involved in wrongdoing

This guide provides implementation guidance that defines principles and points of focus⁶ 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, 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 needs to 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 process. For example, it addresses fraud risk management roles and responsibilities, fraud risk management considerations for smaller organizations, data analytics employed as a part of fraud risk management, and managing fraud risk in the government environment.

⁴ For purposes of this guide, the authors developed this practical definition. 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.

⁵ 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.

⁶ Per COSO's *Internal Control — Integrated Framework* (May 2013) (2013 COSO Framework), Relevant Principles represent fundamental concepts associated with components of internal control. Points of Focus are important characteristics of principles.

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

COSO revised its 1992 *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 2013 COSO Framework's 17 internal control principles.⁷ The correlation between the fraud risk management principles and the 2013 COSO Framework's internal control components and principles is as follows:



⁷ The 2013 COSO Framework's 17 internal control principles have been adopted by the U.S. federal government in the *Standards for Internal Controls in the Federal Government*, issued by the Comptroller General of the United States. The Federal Managers' Financial Integrity Act of 1982 requires federal agencies to follow the Comptroller General's standards. In addition, the Government Accountability Office (GAO) has issued a *Framework for Managing Fraud Risks in Federal Programs*, which was developed based on leading practices as a tool for federal agencies to use in developing Fraud Risk Management Programs. [See [gao.gov/assets/680/671664.pdf](https://www.gao.gov/assets/680/671664.pdf).]

The most obvious correlation between these two sets of principles is 2013 COSO Framework principle 8 (The organization considers the potential for fraud in assessing risks for the achievement of objectives) and fraud risk management 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). In addition, as the above exhibit displays, all of the 2013 COSO Framework and fraud risk management principles correlate and support each other.

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 Assessment

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 illegal acts (including

corruption). 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 2013 COSO 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.



Control
Activities

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 non-compliance

and allegations involving 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.



Information &
Communication

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 process. 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 2013 COSO 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.



Monitoring
Activities

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.

Effective Fraud Risk Management

The 2013 COSO Framework clarifies that for a system of internal control to be effective, each of its 17 principles is present, functioning, and operating in an integrated manner.

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 2013 COSO Framework and can serve as best practices guidance for organizations to follow in performing a fraud risk assessment.

Recommended Use of the Fraud Risk Management Guide

The guide is designed for use by any organization regardless of its status as public, private, government, academic, or not-for-profit; its relative size; or its industry. Obviously, each specific implementing organization will adapt these fraud risk management principles. In particular, smaller organizations and owner-managed organizations without governing boards can adapt the guide to their particular circumstances. Governments have much different governance structures, with elected officials, branches of government, and high-level political appointees.

The terms identified in these chapters are generic and are adaptable to the implementing organization. For example, and as noted previously, the guide uses the terms “board” or “governing board” to refer to the body exercising overall management oversight and organizational governance, regardless of what such a body is called within a particular organization.

This guide’s authors recommend that organizations implementing the 2013 COSO Framework implement this guide as a separate, compatible, and more comprehensive process for specifically assessing the organization’s fraud risk as part of a broader Fraud Risk Management Program or process. That approach, *in addition to the fraud risk assessment*, 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 2013 COSO Framework.

This rigorous approach results in an ongoing, comprehensive fraud risk management process as follows:

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 internal control assessment may not thoroughly examine and identify possibilities for intentional 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 process provides greater assurance that the assessment's focus remains on intentional acts.

The comprehensive 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 2013 COSO Framework's results to yield more robust prevention and detection mechanisms.

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 any incidents of fraud or suspected fraud. The board challenges management and asks the tough questions, as necessary. It seeks input from internal auditors, independent auditors, external reviewers, and legal counsel and utilizes these resources as needed to investigate any issues.

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 2013 COSO 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 2013 COSO Framework.

Internal Audit

Internal auditors review their internal audit plans and how the plans are applied to the entity's Fraud Risk Management Programs in connection with implementation of this guidance. Internal auditors will review this guide and consider possible implications of changes to the entity's fraud risk program on audit plans, evaluations, and any reporting on the entity's fraud risk management and system of internal control.

Independent Auditors

In many situations, an 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 2013 COSO 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.

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

With the presumption that the guide attains broad acceptance, its concepts and terms will find their way into university curricula.