FRAUD RISK MANAGEMENT GUIDE

Second Edition

COSO

Committee of Sponsoring Organizations of the Treadway Coåmmission

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 and ACFE also thank Sergio Analco and Laura Hymes for their outstanding design and editorial expertise.

COSO Board Members

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

March 2023 | Research Commissioned by

COSO

Committee of Sponsoring Organizations of the Treadway Coåmmission

Co-published by

ACFE

Association of Certified Fraud Examiners

ISBN: 978-1-95515-943-2 ACOSOFRM23D
eBook: 978-1-95515-942-5 ACOSOFRM23E

Design and layout: SergioAnalco.com

coso.org

CONTENTS PAGE

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.

However, 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 *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 vii to ix).

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

David Coderre
CAATS

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

John D. Gill
ACFE

Sandra K. Johnigan, *Co-Chair*
Johnigan, PC

Andi McNeal
ACFE

Linda Miller
Audient Group, LLC

Lynda Schwartz
University of Massachusetts Amherst

Jeffrey Steinhoff
Formerly KPMG and GAO

Pamela Verick
Protiviti

Vincent Walden
KonaAI

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

Tim Berichon
Institute of Internal Auditors

Sonia Boguslavsky
Bank of Israel

Dr. El-fred Boo
Nanyang Technological University

Mike Carter
Bittrex, Inc.

Margot Cella
Center for Audit Quality

Dr. Todd DeZoort
The University of Alabama

Scott Hilsen
Cox Automotive, Inc.

Robert Hirth
Protiviti

Robert Hogan
Hogan Forensics

Ryan Hubbs
Schlumberger

Jonathan T. Marks
Baker Tilly US, LLP

Anne Mercer
Institute of Internal Auditors

Rhod Newcombe
Brit Insurance

Joseph Palmar
Palmar Forensics

Brad Preber
Grant Thornton

Katherine Robinson
Sterling Bank & Trust, FSB

Valerie Scarantino
UGI Corporation

Paul Sobel
COSO Chairman

Dr. Robert Tennant
Institute of Management Accountants

Lucy Wang
Center for Audit Quality

Elizabeth Zachem Woodward
Dean Dorton

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

Michael Birdsall
Comcast Corporation

Toby Bishop
Formerly ACFE, Deloitte

Margot Cella
Center for Audit Quality

David Coderre
CAATS

David L. Cotton, *Chair*
Cotton, A Sikich Company

James Dalkin
GAO

Ron Durkin
Durkin Forensic, Inc.

Bert Edwards
Formerly State Department

Frank Faist
Charter Communications

Eric Feldman
Affiliated Monitors, Inc.

Dan George
USAC

John D. Gill
ACFE

Leslye Givarz
Formerly AICPA, PCAOB

Cindi Hook
Comcast Corporation

Sandra K. Johnigan
Johnigan, PC

Bill Leone
Norton Rose Fulbright

Andi McNeal
ACFE

Linda Miller
Audient Group, LLC

Kemi Olateju
General Electric

Chris Pembroke
Crawford & Associates, PC

J. Michael Peppers
University of Texas

Kelly Richmond Pope
DePaul University

Carolyn Devine Saint
University of Virginia

Jeffrey Steinhoff
Formerly KPMG and GAO

William Titera
Formerly EY

Michael Ueltzen
Ueltzen & Company

Pamela Verick
Protiviti

Vincent Walden
KonaAI

Bill Warren
PwC

Richard Woodford
U.S. Coast Guard Investigative Service

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 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.

INTRODUCTION

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 demonstrates 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**[1] (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 fraud[2] 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] Throughout this Guide, words or terms shown in bold font indicate that these words or terms are defined in the Glossary, Appendix A.

[2] 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 directors[3] 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 2023 *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 2023 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.

[3] 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, crypto-currency, 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 2023 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

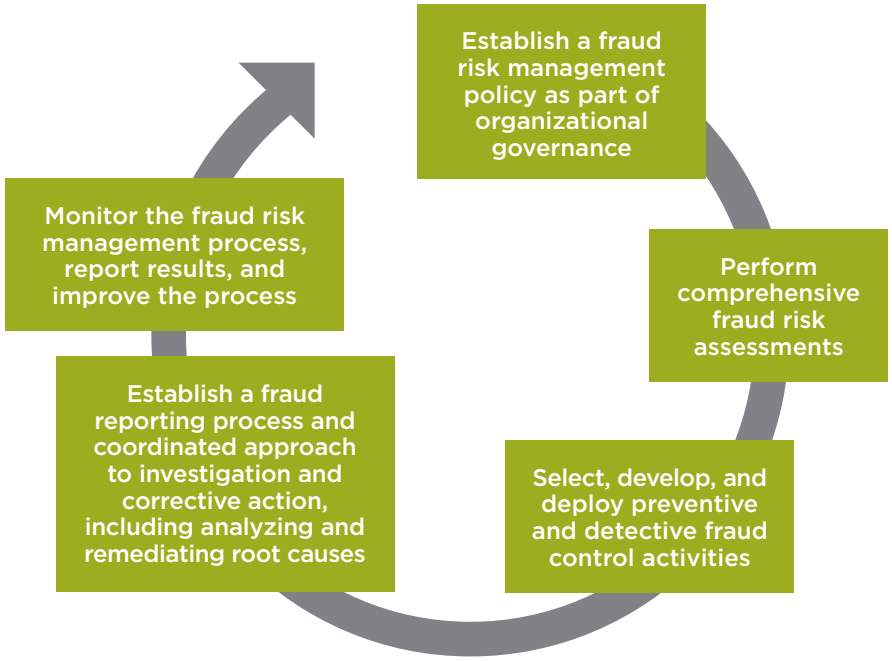
The Guide also defines important terminology (see Appendix A), explains key roles and responsibilities (see Appendix B), and describes how it can be applied to smaller organizations (see Appendix C).

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



The first approach focuses only on the second step above, but will still assist in addressing COSO 2013 IC Framework Principle 8.

This Guide's authors recommend the second approach (applying all five of the above steps). The second 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 process provides greater assurance 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.

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 shown in Figure 2.

Figure 2. Relationship Between the COSO 2013 IC Framework's Five Components and 17 Internal Control Principles and this Guide's Five Fraud Risk Management Principles

The most obvious correlation between these two sets of principles is COSO 2013 IC Framework Principle 8 and Fraud Risk Management Principle 2. But, as Figure 2 displays, all of the COSO 2013 IC Framework and fraud risk management principles correlate with and support each other.

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).

This Guide contains five chapters that correspond to the five fraud risk management principles:

Control Environment

Chapter introduces **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.

Risk Assessment

Chapter introduces **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.

Control Activities

Chapter introduces **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.

Information & Communication

Chapter introduces **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.

Monitoring Activities

Chapter introduces **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.

For a fraud risk management system to be effective, each of these fraud risk management principles is present, functioning, and operating in an integrated manner.

Each chapter of this Guide contains a chapter summary, explanation of how the particular fraud risk management principle correlates with the COSO 2013 IC Framework's principles, and points of focus. Consistent with the COSO 2013 IC Framework's points of focus, these fraud risk management points of focus are important characteristics of each fraud risk management principle. Management may determine that some of these points of focus are not suitable or relevant and may identify and consider others based on specific circumstances of the entity. *Points of focus may assist management in designing, implementing, and conducting fraud risk management activities and in assessing whether the relevant principles are, in fact, present and functioning.* (Adapted from COSO 2013 IC Framework.)

The Guide's appendices and the additional resources at the ACFE Tools site contain additional samples, prototypes, analytics procedures, and practice aids to consider using in fully implementing a comprehensive Fraud Risk Management Program and its processes.

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, these fraud risk management principles would be adapted to each specific implementing organization. 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 charged with governance, overall management oversight, and organizational governance, regardless of what such a body is called within a particular organization.

CHAPTER 1. FRAUD RISK GOVERNANCE

Chapter Summary

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 is the discipline that addresses the assessed risks to achieving the organization's objectives and goals.

This chapter addresses governance and the internal control environment as they affect managing fraud risk and protecting the organization and its stakeholders from **asset misappropriation**, fraudulent financial reporting, and corruption.

The board of directors and senior management, within their respective governance and oversight responsibilities, establish the tone at the top regarding the importance of fraud risk management based on the foundation of expected standards of ethical conduct.

Management reinforces these expectations at each level throughout the organization. An important step in communicating the organization's commitment is the assignment of the overall responsibility for fraud risk management to a single senior executive. While this executive provides a central point of focus, this does not reduce the responsibility of everyone in the organization to be sensitive to fraud risk.

The board of directors and all levels of management work to create a culture of compliance. They are expected to lead by example, exhibiting integrity and ethical values and developing a philosophy and operating style for the organization that does not tolerate fraudulent behavior or noncompliance with laws and regulations. To accomplish this, they take into account the reasonable expectations and objectives of the organization's various stakeholders. Achieving this type of control environment requires an ethical lens in all managerial and operational processes and not just in the boardroom.

As part of governance, the board and senior management promote a strong system of internal control that supports the achievement of the organization's business objectives, which is part of managing fraud risk.

Fraud risk governance is also an important aspect of organizational compliance with laws, rules, and regulations. Punishments of corporate offenders can be less severe for organizations that have compliance and ethics programs that are effective. According to the 2021 USSC Guidelines Manual (Section 8B2.1(2)), such programs shall be reasonably designed, implemented, and enforced so that they are generally effective in preventing and detecting criminal conduct.

Fraud Risk Governance Principle

This chapter addresses Principle 1 of a Fraud Risk Management Program. Principle 1 states:

Control Environment

Chapter introduces **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.

Relationship to the COSO 2013 Internal Control Framework

In addition to the requirement to assess fraud risk in COSO 2013 IC Framework Principle 8 (*The organization considers the potential for fraud in assessing risks to the achievement of objectives*), each component and principle of the COSO 2013 IC Framework is relevant to the consideration of the risk of fraud. Therefore, the principle discussed in this chapter about fraud risk governance mirrors the COSO 2013 IC Framework's control environment principles. The COSO 2013 IC Framework, when read in conjunction with this chapter on fraud risk governance, provides informative context regarding the topic of this chapter.

Figure 3. Fraud Risk Management Principle 1 Correlates with the COSO 2013 IC Framework's Control Environment Components and Principles

COSO Framework Components and Principles		Fraud Risk Management Principle
Control Environment	1. The organization demonstrates a commitment to integrity and ethical values.	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.
	2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
	3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
	4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
	5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	

The COSO 2013 IC Framework's control environment principles are broadly designed to help ensure that the organization makes a commitment to a tone at the top that supports an effective internal control system with respect to the mitigation of risks to the achievement of objectives. Fraud Risk Management Principle 1 focuses on establishment of a governance program related specifically to fraud risk. Each of the five COSO control environment principles is consistent with and supportive of Fraud Risk Management Principle 1.

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- **Makes an Organizational Commitment to Fraud Risk Management** — The board of directors and senior management initiate the Fraud Risk Management Program by establishing an organizational commitment to deter, prevent, and detect fraud.
- **Supports Fraud Risk Governance** — The board of directors, senior management, and middle management make an organizational commitment to fraud risk management as a key element of organizational governance.
- **Establishes a Comprehensive Fraud Risk Management Program** — The board of directors and management provide a solid foundation of fraud risk management by establishing a comprehensive Fraud Risk Management Program.
- **Establishes Fraud Risk Governance Roles and Responsibilities throughout the Organization** — The board of directors and senior management identify the roles and responsibilities of all personnel as they relate to fraud risk governance.
- **Documents the Fraud Risk Management Program** — The board of directors and senior management ensure that the Fraud Risk Management Program is thoroughly documented and updated on a regular basis.
- **Communicates Fraud Risk Management at all Organizational Levels** — The board of directors and senior management support the ongoing effectiveness of the Fraud Risk Management Program by maintaining and communicating an ongoing focus on fraud deterrence, prevention, and detection throughout the organization.
- **Uses Data Analytics to Support Fraud Risk Governance** — The board of directors and management enhance effective fraud risk governance through the use of data analytics and reporting.

Makes an Organizational Commitment to Fraud Risk Management

The fraud risk management control environment is influenced by a variety of internal and external factors that constitute an organization's culture. According to the COSO 2013 IC Framework (Chapter 5):

> **Organizational culture** supports the control environment insofar as it sets expectations of behavior that reflects a commitment to integrity and ethical values, oversight, accountability, and performance evaluation. Establishing a strong culture considers, for example, how clearly and consistently ethical and behavioral standards are communicated and reinforced in practice. As such, culture is part of an organization's control environment, but also encompasses elements of other components of internal control, such as policies and procedures, ease of access to information, and responsiveness to results of monitoring activities. Therefore, culture is influenced by the control environment and other components of internal control, and vice versa.

The Effect of Ethics

Effective boards and organizations address issues of ethics and the effects of ethical behavior on business strategy, operations, and long-term survival. The level of board and organizational commitment to these objectives can vary, and as a result can affect the level of fraud risk that an organization can face.

Organizational culture is influenced by the fraud risk management control environment, and the fraud risk management control environment is influenced by the organization's culture. Successful entities have a strong correlation between the two.

In general, ethics considerations go beyond mere compliance programs. When entities make ethics considerations a priority, the long-term benefits of their actions outweigh the related costs. For instance, effective business ethics programs can serve as the foundation for deterring, preventing, and detecting fraudulent and criminal acts. These ethics programs create an environment in which making the right decision is implicit. By contrast, compliance programs sometimes focus only on preventing wrong decisions that can lead to legal and regulatory violations.

It is always best to think of legislative and regulatory requirements as the minimum standards or floor and not the ceiling of doing the right thing, and to instill that philosophy in the fiber of the organization's culture.

Both ethics considerations and well-directed compliance programs are important foundational components of effective fraud risk management. The inclusion of fraud risk management is also key to corporate governance.

Application of ERM Concepts

Risk appetite and **risk tolerance** are fundamental risk management concepts. The concepts were introduced in the 2004 ERM Framework. The COSO 2017 ERM Framework continues to use the term risk appetite. However, the term risk tolerance was changed to **tolerance**. In applying the ERM, it is important to be aware that addressing fraud risk is an appropriate component of these ERM concepts.

Risk appetite and tolerance are established at the broader enterprise risk management level. Principle 7 of the COSO 2017 ERM Framework states, "The organization defines risk appetite in the context of creating, preserving, and realizing value." That principle makes clear that:

> *There is no standard or "right" risk appetite that applies to all entities. Management and the board of directors choose a risk appetite with an informed understanding of the trade-offs involved. Risk appetite may encompass a single depiction or several depictions that align and collectively specify the acceptable types and amount of risk.*

The COSO 2017 ERM Framework describes tolerance for risk as compared to risk appetite as tactical and focused and notes that it is intended to be evaluated as such throughout the entity. Therefore, an effective Fraud Risk Management Program is designed to incorporate the entity's defined tolerance for the risk of fraud at various levels throughout the entity.

Fraud risk tolerance is a subset of an organization's overall risk tolerance. It is the level of residual fraud risk that an organization is willing to accept, i.e., the risk that a fraudulent event or transaction will occur and not be detected in a timely manner. Fraud risk tolerance recognizes that it is not possible to eliminate all fraud risk in organizations. A company's decision to tolerate that its systems are not designed to prevent or detect all frauds, no matter how small, is not inconsistent with an announced policy of a zero tolerance for fraud that is detected.

Fraud risk tolerance provides the framework for the organization to appropriately address fraud risk mitigation as described in Chapter 2. Such a commitment to managing fraud risk within the entity's risk parameters supports the organization's objectives, mission, and values.

Tone at and Conduct from the Top

One of the most important elements of effective fraud risk management is the tone at and conduct from the top of the organization. Organization leadership has a responsibility to lead by example to ensure that all personnel and all business partners understand that the organization is serious about promoting ethical behavior and is committed to deterring, preventing, and detecting fraud. Further, how management reacts to instances of fraud can send a powerful message inside and outside the organization and act as a strong deterrent to fraudulent behavior.

A primary step in setting the tone from the top is to have a policy regarding the organization's standards of business conduct that reflects the commitment of the organization and its board of directors, officers, executives, and all personnel to conduct business according to the highest standards of integrity and ethics.

Making business partners, including affiliates, contractors, subcontractors, vendors, and others who come into contact with the organization aware of the organization's standards of business conduct strengthens the commitment to integrity and ethics. Emphasizing these efforts in stakeholder communications is an important part of such a program.

Other factors that demonstrate a strong culture of honesty, high integrity, and ethics in organizations include creating positive work environments for employees, hiring and promoting the appropriate employees, training their employees, requiring employees to confirm their understanding of the organization's code of conduct, and disciplining employees appropriately and consistently regardless of their positions within the organization.

In terms of controls, the organization's commitment to a strong tone at and conduct from the top can be considered part of the entity's informal or soft controls, whereas internal controls implemented at the operational and transaction levels (such as **segregation of duties**, reconciliations, and documentation) are formal or hard controls. The key importance of soft controls is that hard controls cannot anticipate and cover every eventuality. Hence, the existence of well-established soft controls — such as the tone at and conduct from the top — can lead to ethical decisions and actions in cases where hard controls are lacking for a particular situation.

Supports Fraud Risk Governance

To set the appropriate fraud risk management tone, the board of directors first ensures that the board itself is governed properly. This encompasses all aspects of governance, including independent-minded board members who:

- Exercise control over board information, agendas, and access to management and outside advisers
- Independently and objectively carry out the responsibilities of the governance, compensation, and audit committees, and any other specific board-directed committees

The board is responsible for ensuring that management designs effective fraud risk management policies enterprise-wide, including policies that encourage ethical behavior and empower employees, customers, and vendors to insist that those standards are met every day. In addition to being independent and objective, the board:

- Has a thorough understanding of what constitutes fraud and corruption
- Sets the appropriate tone at the top in its own independent practices and through the chief executive officer's (CEO's) job description, evaluation, and succession-planning processes
- Maintains oversight of the fraud risk assessment and compliance process
- Evaluates management's identification of fraud risks, including overseeing the internal controls over financial reporting established by management
- Assesses the risk of fraud by management, including the risk of management's override of controls
- Ensures that controls are designed and functioning to deter, prevent, and detect fraud by management
- Establishes and ensures effective oversight of a competent, independent, and objective internal audit function
- Supports internal audit's approved annual plan and ensures that internal audit has adequate skills and resources, fraud-knowledgeable employees, as well as unfettered access to information, data, and employees, taking into consideration certain country or industry regulations about data privacy
- Ensures that internal audit has unrestricted access to the board or a committee of the board (usually the audit committee)
- Receives and considers reports from internal audit, including its assessment of the fraud risk program and residual fraud risk exposures
- Maintains oversight of adequate cybersecurity and data governance (the implications of which could impact reputational risk and compliance in addition to impeding overall strategic goals)
- Ensures that employees have access to the board, audit committee, and internal audit
- Empowers a committee of the board (usually the audit committee) to focus on fraud deterrence, prevention, and detection
- Is fully informed about and takes appropriate action regarding instances of fraud that occur within the organization, in particular, regarding instances involving senior-level employees or instances in which significant internal control issues are uncovered

The board also documents these responsibilities and communicates them appropriately throughout the organization. It also ensures that the organization has sufficient resources, including those required for implementing and maintaining a Fraud Risk Management Program and for retaining outside advisors and counsel, as necessary.

Establishes a Comprehensive Fraud Risk Management Program

An organization's Fraud Risk Management Program includes broad principles that guide personal conduct and does not attempt to catalog every law or policy that may apply. Not all employees encounter all aspects of the Fraud Risk Management Program in their everyday duties. However, it is vital that everyone knows and understands the program and complies with both its legal aspects as well as its intents. It is also important that the fraud risk management policy that documents the Fraud Risk Management Program be in a format that is searchable and formatted for easy reference, including being translated in local languages when applicable. A key concept to engender is substance over form in always doing the right thing.

Organizations with the appropriate focus on fraud deterrence and fraud prevention ensure that their fraud risk management policies emphasize that ethics and honesty are taken very seriously, especially at the highest levels of the organization.

A fundamental tenet of any Fraud Risk Management Program is for employees to understand that the organization does not tolerate fraudulent behavior in any form (regardless of an individual's position within the company), whether it is at the level of bribing foreign officials (violation of federal laws), "cooking the books" (fraudulent financial reporting), falsifying travel and expense statements (**misappropriation** of assets), or any other fraudulent act. No matter how talented individuals are or how high their positions are in the organization, if they are detected committing fraud, but avoid any serious consequences, the organization is taking on an unacceptable risk. Note that such a zero-tolerance policy for detected fraud does not mean the organization needs to design a fraud risk management approach that attempts to prevent or detect *all* frauds regardless of significance. That will be affected by its risk tolerance.

One Size Does Not Fit All

There is no "one-size-fits-all" Fraud Risk Management Program. Different organizations have different objectives, operate in different environments and conditions, and have varied fraud risk profiles. Every organization will perform a tailored fraud risk assessment that is structured to relevant fraud risk scenarios for that particular organization. For each organization, anti-fraud activities will be proportional to the risks.

Identification of the Process to Address Violations or Potential Violations

An effective Fraud Risk Management Program clearly identifies the process that occurs when violations or potential violations surface. The Fraud Risk Management Program includes the development of reporting mechanisms to address identified potential or actual fraud, as well as the method to disclose the existence of such reporting mechanisms.[4]

Individuals or committees at the appropriate level uniformly evaluate violations and potential violations of the Fraud Risk Management Program. Once violations or potential violations are disclosed through the reporting mechanism, there are several available decision paths, including:

- Management may determine that there is no conflict with the organization's policies in the situation described
- Management may decide that there is a potential for conflict with the organization's policies and may impose certain constraints on the party involved to manage the identified risk and to ensure there is no significant opportunity for a policy violation to arise
- Management may assert that there is a conflict with the organization's policies and require the involved party to terminate the activity or leave the organization
- Management may decide that civil or criminal legal actions should be initiated

The organization will also have a process for addressing potential violations by members of senior management or board members. In such cases, oversight by the board or a subset or special committee of the board may be appropriate. In some circumstances, it might be necessary to notify outside parties, including law enforcement and regulators, of actual or suspected improper activity. Prior to notifying anyone, consult with competent legal counsel.

Establishes Fraud Risk Governance Roles and Responsibilities throughout the Organization

Personnel at all levels of the organization have roles and responsibilities with respect to fraud deterrence, prevention, and detection. Board members, internal auditors, compliance professionals, investigators, managers, specialists, and other team members are all important when it comes to fraud risk management.

It is critical to the success of a Fraud Risk Management Program for one executive-level member of management to be assigned overall responsibility for fraud risk management and to report to the board periodically. He or she is at a high enough organizational level to ensure that the Fraud Risk Management Program is taken seriously and implemented fully. This executive-level person is familiar with the organization's fraud risks and process-level controls and is held responsible for the design and implementation of the processes used to help ensure compliance, reporting, and investigation of alleged violations. It is also appropriate to designate a board member or committee that has overall responsibility for investigating allegations of wrongdoing by members of management.

Those charged with governance, including the audit committee of the board, oversee the Fraud Risk

[4] See AICPA Guide to Investigating Business Fraud Chapter 5, The First 48 Hours of an Investigation, Box 5-2: Company Playbook Response Attribute Drivers.

Management Program, address the risk of **management override** of controls, and respond to allegations of wrongdoing by management.

At a minimum, the roles and responsibilities of all personnel are formally documented as part of the organization's Fraud Risk Management Program.

A formalized Fraud Risk Management Program is part of the framework that enhances the likelihood that the fraud risk management policy is more than just a documentation of compliance activities. Rather it serves as a guidepost about the expectations of the board, senior management, and everyone in the organization regarding fraud-related matters.

Fraud risk management policies include communicating and documenting ethical expectations for executives, i.e., those setting the tone at the top.

In many organizations, internal audit may take the lead on fraud risk assessments due to their understanding of relevant risks, knowledge of process flows, understanding of key control frameworks, and **professional skepticism**. Management, however, retains the responsibility for assuring that the Fraud Risk Management Program is carried out under the oversight of those charged with governance. Open, thorough, and timely communications among all parties with key roles in fraud risk management are critical.

Appendix B contains a more detailed discussion of fraud risk management roles and responsibilities. Appendix C discusses fraud risk management considerations for smaller organizations.

Who Owns Fraud Risk Management?

Beyond the importance of assigning the overall responsibility for fraud risk management to an executive-level member of management, the front-line responsibility for *implementing* fraud risk management can vary from organization to organization.

Considering the Institute of Internal Auditors' *Three Lines Model* can be helpful. Under that model, there are three lines related to risk management and control:

- **1st line** roles involve the provision of products/services to client, including managing risk.
- **2nd line** roles involve expertise, support, monitoring, and challenge on risk-related matters.
- **3rd line** roles are with internal audit, providing objective assurance and advice, independent of the management lines.

Although all three lines report administratively to an appropriate member of senior management, a best practice is for the 3rd line, internal audit, to also have a direct, functional reporting line to those charged with governance (e.g., the audit committee in publicly-traded companies). Regardless of where the implementation responsibility is assigned, *it is clear that all three lines will be involved in fraud risk management*. It is important to note, however, that fraud risk management is, by its nature, intended to be preventive and detective. Thus, the 1st and 2nd lines will have more of a role, because they implement preventive and detective controls, whereas the 3rd line's role is providing independent and objective assurance and advice to senior management and the board on the adequacy and effectiveness of controls, including those related to fraud.

There is no single best answer. An organization's Fraud Risk Management Program will make clear who has overall responsibility and who has implementation responsibility and will clearly delineate the responsibilities and authorities assigned.

Documents the Fraud Risk Management Program

The Fraud Risk Management Program supports the design and implementation of a comprehensive and coordinated approach to fraud risk management. This policy is documented and updated based on an organization's current risk profile and current experiences.

Although an organization's standards of business conduct provide the necessary backdrop for the importance of conducting business in an ethical manner, they are not expected to contain the complete range of subjects necessary for an effective Fraud Risk Management Program. Consequently, a separate Fraud Risk Management Program includes documentation of all aspects of the organization's Fraud Risk Management Program.

It is the organization's prerogative, with oversight from the board, to determine the type and format of documentation for its Fraud Risk Management Program. Considerations include:

- Providing a stand-alone comprehensive document addressing in detail all aspects of fraud control activities vs. an integrated document that incorporates other policies or procedures based on the individual components of a Fraud Risk Management Program
- Developing a brief strategy outline emphasizing the attributes of fraud control activities and leaving the design of specific policies and procedures to those responsible for business functions within the organization
- Providing defined, proactive processes and control activities to deter, prevent, and detect fraud and identifying the personnel who will execute the activities and maintain the records that verify that those processes and controls have been properly executed
- Providing a strategy for proactively using data analysis activities to assess areas of high fraud risk and to monitor fraud mitigation activities and controls
- Providing a compilation of plans developed by divisions or subsidiaries

While each organization considers its size and complexity when determining what type of documentation is most appropriate, a best practice is to have a formal Fraud Risk Management Program that contains components of all of the chapters in this document.

The Importance of Fraud Awareness Training

Fraud awareness is key to the effectiveness of a Fraud Risk Management Program. If employees, management, and those charged with governance do not understand fraud, it will be difficult for them to:

- Identify potential fraud risks in the organization
- Report potential fraudulent concerns through the organization's reporting mechanisms
- Establish adequate mitigating measures for fraud risks
- Effectively investigate fraud allegations and implement necessary corrective measures

Heightened fraud awareness throughout the organization will ensure that employees:

- Remain vigilant for signs of fraud and respond appropriately
- Understand their duty to report indications of potential fraud (In some countries, it is illegal to knowingly facilitate fraudulent activities or permit them to continue)
- Do not attempt to confront or investigate suspected perpetrators

The board of directors and members of management at appropriate levels summarize their commitments to a Fraud Risk Management Program in a short document (such as an email or letter) that they make available to all employees, vendors, and customers and, in the case of governmental organizations, to the public and legislative bodies. This summary document stresses the importance of fraud risk mitigation, acknowledges the organization's vulnerability to fraud, and establishes the responsibility for each person within the organization to support fraud deterrence, prevention, and detection activities. The document is endorsed or authored by a senior executive or board member and reissued periodically. The organization ensures that all employees receive this important document by tracking employee acknowledgements of their receipt and their understanding of this information.

Although this type of communication is important, many organizations will augment this written communication by providing a focused fraud training course that is required for all employees because it provides more sustainable results. This enterprise-wide type of training provides a consistent basis for fraud awareness throughout the organization, which is a fundamental pillar of any fraud management effort.

The Fraud Risk Management Program and training define fraud, including the risk of fraudulent financial reporting, misappropriation of assets, and corruption. The policy and training identify potential perpetrators of fraud, provide actual organization-based examples of the types of fraud that could occur (and have occurred), and raise awareness that fraud may be perpetrated by internal or external parties, including members of management.

All personnel and vendors are expected to understand their individual responsibilities related to the Fraud Risk Management Program. The policy and training start by articulating the governance oversight of fraud control (i.e., the role and responsibility of the board of directors and audit committee) as reflected in the board and audit committee charters, where applicable.

The following sample materials related to fraud risk governance can be found at ACFE's Fraud Risk Management Tools web site (ACFE.com/fraudrisktools):

- Fraud Control Policy Framework
- Fraud Policy Decision and Responsibility Matrix
- Combined Code of Business Conduct and Fraud Policy
- Stand-alone Fraud Policy
- Annual Employee Survey

Communicates Fraud Risk Management at all Organizational Levels

The board of directors ultimately holds the CEO accountable for understanding the fraud risks faced by the organization and establishing the requisite system of internal control to help support the achievement of the organization's fraud risk management objectives. The board has a particularly important role in addressing the risk of management override of controls and in responding to allegations of wrong doing by members of senior management.

The board is also responsible for monitoring the effectiveness of the programs — a responsibility that is addressed under a periodic agenda item at board meetings when considering the general risks of the organization. (See Chapter 5 of this Guide for discussion about Fraud Risk Management Program monitoring.)

The board establishes mechanisms to ensure that it is receiving accurate and timely data and information from management, employees, internal auditors, external auditors, and other stakeholders regarding potential fraud occurrences. In its communications with relevant parties, the board assesses the degree to which these parties believe the organization's fraud practices and policies are adequate.

Fraud-aware organizations make the identification, assessment, and implementation of measures to prevent or detect fraud a standing agenda item for boards and key committees, with specific emphasis on emerging threats and areas where current risks may be heightened.

The CEO and senior management are responsible for designing, implementing, conducting, and periodically assessing the structures, authorities, and responsibilities needed to establish accountability for internal control, including fraud risk management and fraud prevention and detection at all levels in the organization.

The Fraud Risk Management Program communicates the organization's risk tolerance considerations and establishes the expectation that suspected fraud will be reported immediately. The organization conveys that it has the right to institute civil or criminal action against anyone who commits fraud. The channels to report suspected fraud issues are clearly defined and may be the same or different for other code of conduct violations.

To encourage timely reporting of suspected issues, the organization communicates the protections afforded to the individual reporting the issue — often referred to as whistleblower protection. It is essential that those reporting misconduct do not subsequently face any form of retaliation. Retaliation or even a perception of retaliation has a chilling impact on whistleblower systems. Retaliation is a serious violation of organizational fraud risk requirements and should be handled accordingly. (See Chapter 4 of this Guide for a more complete description of the whistleblower process.)

A **whistleblower system** (both a formal "hotline" system as well as other related processes) is an essential component of a Fraud Risk Management Program. An effective Fraud Risk Management Program includes a thorough explanation of this process, which is especially important from the perspective of the board (typically the audit committee) about what types of fraud get reported to the board.

In many organizations, allegations of fraud and ethical violations arise through a variety of sources, including human resources, the whistleblower reporting system, data analytics, corporate security, vendors, auditors, and regulators. The Fraud Risk Management Program clarifies the types of events requiring a detailed explanation to the board and the types of violations to be tracked and reported in aggregate (for monitoring purposes and trend identification). All of those events and violations are not necessarily communicated to the audit committee in detail. Given the importance of the processes associated with gathering and reporting various statistics to the audit committee, many organizations have asked their internal audit group to provide assurance and advice on the reliability of data gathering and reporting for completeness, accuracy, and follow through.

When fraud allegations arise or when an investigation uncovers improper behavior or transactions, the Fraud Risk Management Program reflects the need to conduct a remediation analysis to identify the control weakness that failed to prevent or timely detect the fraudulent act. The remediation analysis leads to correction and strengthening of any identified control deficiencies. As a deterrent, the policy reflects the consequences for fraudulent activity. These consequences may include termination of employment or of a contract and reporting to legal and regulatory authorities.

Senior management also considers sharing, on an organization-wide basis, the results of some key frauds that have taken place in the organization, including the ultimate consequences to the perpetrators (termination/criminal prosecution) to further establish the fraud risk tolerance policy that exists. This action may increase awareness that fraud can, and does, occur in the organization, that there are negative repercussions to the organization and all employees, that fraud is not tolerated in the organization, and that everyone is to be cognizant of fraud indicators and willing to come forward when they first become aware of problems.

Uses Data Analytics to Support Fraud Risk Governance

Demonstrating and strengthening effective fraud risk governance in an organization can be significantly enhanced through the use of data analytics and reporting focused on efficiency and effectiveness of key governance activities. For example, data analytics might address the following questions related to the effectiveness of the organization's governance activities:

- What issues are trending? Mobile "compliance" apps have become a popular element of anti-fraud and compliance policies due to their ease of use and searchability by topic. Data from these apps can be anonymously mined to identify risks and employee training needs. For example, one company found the phrase "What is a conflict of interest?" searched over 5,000 times on its mobile app. Consequently, the company was able to update its policies and training to address company-specific scenarios.
- Are anti-fraud efforts updated based on lessons learned? Data analytics can identify new risks, trends, or policy gaps. Taking a data-driven approach to continuously updating and improving policies and procedures, while also keeping it simple and practical, is a good way to demonstrate effective fraud risk governance.

These examples are consistent with Fraud Risk Management Program Principle 5, explained in Chapter 5.

Once the organization establishes and implements the key elements of fraud risk governance, the next phase of the Fraud Risk Management Program is performance of comprehensive fraud risk assessments. Chapter 2 explains how organizations plan and carry out this next phase.

CHAPTER 2. FRAUD RISK ASSESSMENT

Chapter Summary

Chapter 1 addressed how the organization establishes and implements fraud risk governance. This chapter explains the next important phase of fraud risk management: performing comprehensive fraud risk assessments. With the ever-increasing degree of organizational information being digitized, this chapter will also include examples of how data analytics can be considered when performing fraud risk assessments.

Every organization faces a variety of fraud risks from internal and external sources. Organizations have operating, reporting, and compliance objectives, and management is responsible for identifying the internal and external fraud risks that could prevent the organization from achieving those objectives.

A fraud risk assessment is a dynamic and iterative process for identifying and assessing fraud risks relevant to the organization. This assessment addresses the risk of fraudulent financial reporting, fraudulent non-financial reporting, asset misappropriation, and other illegal acts (including corruption). Organizations can tailor this approach to meet their individual needs, complexities, and goals.

The initial fraud risk assessment forms the basis for how the organization manages its fraud risks. Subsequent fraud risk assessments address environmental, operational, and organizational changes and refine and improve the management of fraud risks.

Regulators, professional standard-setters, and law enforcement authorities have emphasized the crucial role that fraud risk assessment plays in developing and maintaining effective Fraud Risk Management Programs and controls.[5] This chapter provides guidance for conducting a fraud risk assessment.

Fraud risk management control activities consider both the potential fraud schemes and the individuals within and outside the organization who could be the perpetrators of each scheme. If a potential fraud scheme is collusive, i.e., if it involves more than one person, it is important for preventive controls to be augmented by detective controls because **collusion** may negate the control effectiveness of the segregation of duties in an organization. (Chapter 3 discusses designing effective preventive and detective controls in more detail and explains how the development of these control activities is driven by and linked to the risk assessment.)

Fraud entails intentional misconduct that is designed to evade detection. As such, the fraud risk assessment team engages in strategic reasoning to anticipate the behavior of a potential fraud perpetrator.[6] Strategic reasoning requires a skeptical mind-set and involves asking questions such as:

- How might a fraud perpetrator exploit weaknesses in the system of controls?
- How could a perpetrator override or circumvent controls?
- Who might have a motive or incentive to commit fraud?
- Given identified fraud risks, which controls are critical to preventing fraud?
- What controls might be subject to fraudulent attacks?
- What are the risks of management override of controls, conflicts of interest, or wrongdoing by members of management or governance?
- What new types of fraud trending in the media might affect the organization?

Such questions are also considered in the context of individuals and organizations external to the organization. What are the opportunities within the organization that could allow such fraud?

Additionally, fraud risks evolve as organizations grow and change and as technology and the operating environment change. Therefore, it is important for a fraud risk assessment to evolve and to be updated periodically to reflect both internal changes, such as expansion of the organization's mission, newer data analytics capabilities to identify risk, changes in personnel, changes in processes (such as receiving inventory in offsite warehouses), or updates to information systems and controls, and external changes in the environment in which the organization operates, such as new cybersecurity risks.

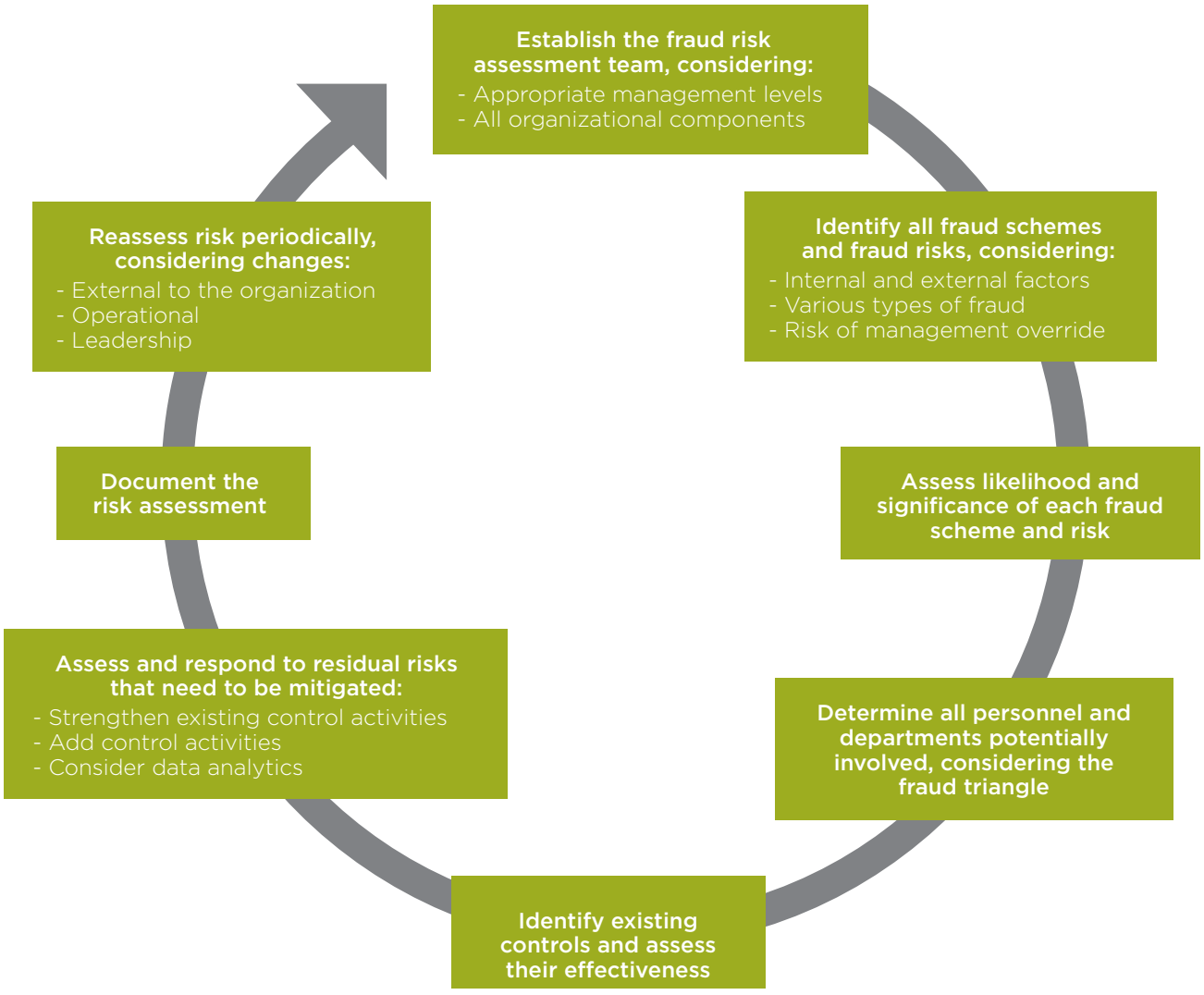
---

[5] SEC, 17 CFR 241, *Commission Guidance Regarding Management's Report on Internal Control over Financial Reporting under Section 13(b) or 15(d) of the Securities and Exchange Act of 1934; PCAOB AS 2201, An Audit of Internal Control over Financial Reporting That is Integrated with an Audit of Financial Statements; IIA, Practice Advisory 1210-A2-1: Auditor's Responsibilities Related to Fraud Risk Assessment, Prevention, and Detection; AICPA, AU-C sec. 240, Consideration of Fraud in a Financial Statement Audit* [See aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00240.pdf.]; and International Standards on Auditing (ISA) No. 240, *The Auditor's Responsibility Related to Fraud in an Audit of Financial Statements* [See ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf].

[6] T. Jeffrey Wilks and M. F. Zimmerman, *Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud*, Accounting Horizons, 18 3 (September 2004).

The graphic below illustrates the fraud risk assessment explained in this chapter.

Figure 4. Fraud Risk Assessment Process



Fraud Risk Assessment Principle

This chapter addresses Principle 2 of a Fraud Risk Management Program. Principle 2 states:

Risk Assessment

Chapter introduces Principle 2

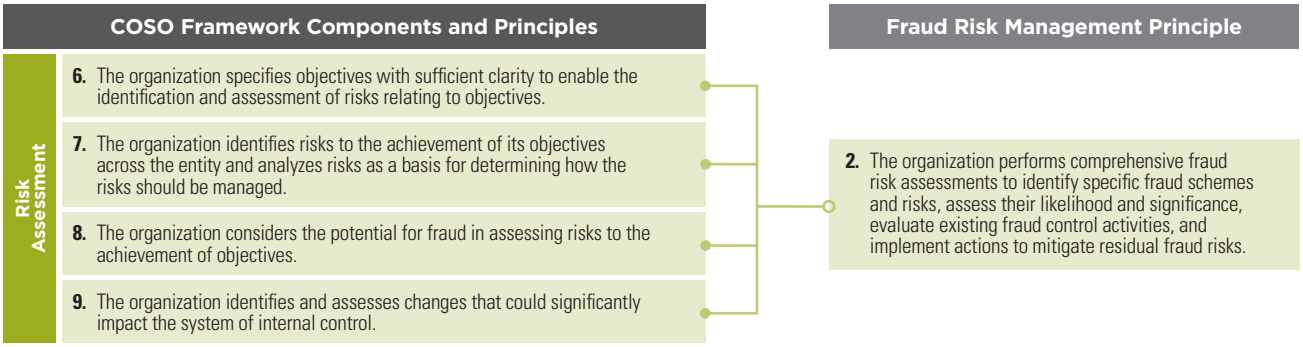
The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

Relationship to the COSO 2013 Internal Control Framework

In addition to the requirement to assess fraud risk in the COSO 2013 IC Framework Principle 8 (*The organization considers the potential for fraud in assessing risks to the achievement of objectives*), each component and principle of the COSO 2013 IC Framework is relevant to the consideration of the risk of fraud. Therefore, the principle discussed in this chapter about performing fraud risk assessments mirrors the COSO 2013 IC Framework's risk assessment principles. The COSO 2013 IC Framework, when read in conjunction with this chapter on performing fraud risk assessments, provides informative context regarding the topic of this chapter.

Fraud risk management Principle 2 correlates to the COSO 2013 IC Framework's components and principles as follows:

Figure 5. Fraud Risk Management Principle 2 Correlates to the COSO 2013 IC Framework's Control Environment Components and Principles



While the COSO 2013 IC Framework's risk assessment Principle 8 specifically emphasizes the need for a fraud risk assessment, the points of focus included within all of the COSO 2013 IC Framework's risk assessment principles are important considerations when conducting an effective fraud risk assessment. This chapter provides insight into how to leverage the relevant points of focus within the risk assessment principles to address fraud risks.

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- **Involves Appropriate Levels of Management —** The fraud risk assessment team includes appropriate levels of management.
- **Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels —** The fraud risk assessment team recognizes that frauds can happen at any level or component of the organization.
- **Analyzes Internal and External Factors —** The fraud risk assessment team considers both internal and external factors and their impact on the achievement of objectives.
- **Considers Various Types of Fraud —** The fraud risk assessment team considers a wide range of possible fraud schemes and exposures.
- **Specifically Considers the Risk of Management Override of Controls —** The fraud risk assessment team understands that catastrophic frauds have been perpetrated by senior members of management overriding existing and otherwise effective controls and focuses on these risks.
- **Assesses the Likelihood and Significance of Risks Identified —** The fraud risk assessment team carefully evaluates the probability that each particular fraud could occur and the potential effects on the organization if that particular fraud occurs.
- **Considers the Fraud Triangle and Other Models to Evaluate the Landscape —** The fraud risk assessment team considers both traditional and current models of fraud.

- **Identifies Existing Fraud Control Activities and Assesses Their Effectiveness** — The fraud risk assessment team identifies and evaluates existing controls for effectiveness to determine residual fraud risks that require mitigation.
- **Determines How to Respond to Risks** — The fraud risk assessment team's ultimate goal is to formulate effective and appropriate responses to specifically identified fraud risks.
- **Uses Data Analytics Techniques for Fraud Risk Assessment and Fraud Risk Responses** — The organization uses data analytics to improve the effectiveness and reliability of the fraud risk assessment.
- **Documents the Risk Assessment** — The organization understands that the risk assessment serves as the central element of the fraud risk management process and ensures that it is carefully and thoroughly documented.
- **Performs Reassessments and Assesses Changes to Fraud Risk** — The organization keeps its fraud risk assessment relevant and effective through periodic updates and by responding to new information and feedback, such as the results of investigations, internal audits, compliance reviews, and regulatory guidance. The fraud risk assessment is updated when business operations and conditions change, such as changes in the external environment, operating models, personnel, leadership, and emerging fraud risks.

Involves Appropriate Levels of Management

The fraud risk assessment team includes the appropriate levels of management and internal and external sources to assess fraud throughout the organization. A risk assessment process requires input from various sources.

Before conducting a risk assessment, senior management identifies a risk assessment team. This team includes individuals from throughout the organization with different knowledge, skills, and perspectives. In addition, the risk assessment relies on a combination of internal and external resources, such as:

- Accounting/finance personnel who are familiar with the financial reporting process and internal controls
- Non-financial business unit and operations personnel who leverage their knowledge of day-to-day operations, customer and vendor interactions, and general awareness of issues within the industry
- Information technology (IT) personnel who understand the strengths and weakness of the various systems utilized by the organization
- Risk management personnel who ensure that the fraud risk assessment process integrates with the organization's enterprise risk management program
- Legal and compliance personnel, in the event the fraud risk assessment identifies risks that give rise to potential criminal, civil, and regulatory liability if the fraud or misconduct occurs
- Members of the internal audit function since they are familiar with the organization's internal controls and monitoring functions and routinely assess fraud risk and provide assurance and advice on significant fraud risks and controls
- Security or other personnel with experience investigating suspected or alleged fraud
- Technical experts in topics such as data analytics and cybersecurity
- If expertise is not available internally, external consultants with expertise in applicable standards, key risk indicators, anti-fraud methodology, control activities, and detection procedures

Management, including senior management, business unit leaders, and significant process owners (e.g., accounting, sales, procurement, and operations), participate in the assessment because they are ultimately accountable for the effectiveness of the organization's fraud risk management efforts and because they have a high-level view and understanding of the organization's operations, strategies, and risks.

The fraud risk assessment team reviews the organization's strategic plan, process maps, and control matrices to understand the population of activities that are potentially exposed to fraud risk. Even when a robust fraud risk assessment was performed in the recent past and there have been no significant known changes to the organization or its internal or external operating environments since then, updating that prior risk assessment is appropriate, because the fraud threat environment is constantly changing.

The risk assessment teams engage in a brainstorming activity to identify the organization's fraud risks. Effective brainstorming involves preparation in advance of the meeting, a leader to set the agenda and facilitate the session, and an attitude that includes openness to ideas regarding potential risks and controls. It can be beneficial to include data analytics personnel in this process, because they can contemplate how data analytics can be applied to mitigate identified fraud risks.

Brainstorming enables discussions of the incentives, pressures, and opportunities to commit fraud; the risks of management override of controls; and the population of fraud risks relevant to the organization. Other risks, such as regulatory and legal misconduct, the effect of IT on fraud risks, and **reputation risk**, are also considerations in the fraud risk identification process. The fraud risk assessment team identifies the areas of the organization that require more detailed fraud brainstorming sessions to properly assess all relevant fraud risks.

For example, an organization with a large manufacturing and distribution component may wish to convene a separate manufacturing and inventory fraud risk assessment team. This team comprises individuals who work in manufacturing and inventory management and in the supporting operations (accounting, IT, and procurement). This focused team is better able to identify and address the specific fraud schemes because personnel that execute processes and controls every day are likely to know the ways in which processes and controls can be overridden or circumvented.

The fraud risk assessment team shares the organization's fraud risk identification information with the board or audit committee and solicits feedback from them. The board also assesses the implications of its own processes with respect to its contribution to fraud risk, including incentives and other pressures that its policies create.

Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels

The organization identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of its objectives. Depending on the size and organizational complexity of the organization, it may need to assemble multiple fraud risk assessment teams to ensure consideration of possible fraud schemes or potential fraud risk exposures throughout the organization.

Each team includes personnel with a detailed working knowledge and understanding of how the organizational unit operates and how it interacts with other organizational units. In a large or complex organization, the overall risk assessment may be the product of many smaller risk assessments under the guidance and direction of a higher-level team of fraud risk management specialists.

Analyzes Internal and External Factors

Risk identification considers both internal and external factors and their impact on the achievement of objectives.

Internal factors include the types of activities the organization normally performs and the processes and controls in place to process and account for those actions. Organizations may carry out similar activities in all the geographies in which they operate, but have vastly different processes or controls in place in different locations. For example, the organization may not have a high-quality IT infrastructure at certain locations, or certain locations may not have enough personnel in place to ensure proper segregation of incompatible duties. Internal factors also include organizational incentives and pressures such as the desire to meet stock price expectations, meet revenue and profit goals, or adhere to budgets.

External factors include the customers and vendors with whom the organization interacts, as well as the business environment in which the organization operates. Examples of external factors to consider are the perceived prevalence of corruption in the different geographies in which the organization operates. The organization may have more specific anti-corruption controls and more frequent monitoring of those controls in countries that have a higher corruption risk. External factors also can include the extent to which individuals or groups may be inclined to disrupt or otherwise interfere with the organization's business, including organized criminal groups that may target the organization.

To be clear, the fraud risk assessment 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, account takeover, social engineering, data breaches, identity theft, and a wide range of corruption schemes.

Considers Various Types of Fraud

To ensure a comprehensive assessment of potential fraud risks impeding an organization based on its identified objectives, management considers various types of fraud that can be committed against or by the organization. These types include fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of assets, and other illegal acts, which include corruption, false claims, and tax and entitlement program fraud.

The fraud risk identification process requires understanding the universe of known fraud risks and the subset of risks specific to the organization. ACFE's Fraud Risk Management Tools web site (ACFE.com/fraudrisktools) has a list of the types of fraud schemes and fraud exposures an organization might encounter. It can serve as a starting point in the risk identification process. This process may also involve obtaining information from external sources, such as industry news; criminal, civil, and regulatory complaints and settlements; as well as organizations, such as the Institute of Internal Auditors, the American Institute of CPAs, AGA (formerly the Association of Government Accountants), the Association of Government Accountants, and the Institute for Internal Controls; and governmental agencies, such the Federal Bureau of Investigation, the Government Accountability Office, the federal inspectors general, the United States Department of Justice, and comparable state-level agencies and international counterparts.

This fraud risk identification process also involves gathering information about potential fraud from internal sources by interviewing personnel and brainstorming with them, reviewing information received from the whistleblower reporting system, and performing analytical procedures. The approach to fraud risk identification needs to be systematic and comprehensive to ensure that no potentially significant areas are overlooked.

The fraud risk identification process includes recognizing that new fraud schemes, and thus new fraud risks, are continually emerging as technologies and business environments evolve and change. An effective approach to fraud risk identification will include monitoring media and other reports about fraud — particularly in the organization's operating arena — to identify new types of fraud and fraud risks. Deep and dark web monitoring is also an effective information channel. Organizations can partner with a cyber threat intelligence provider who specializes in infiltrating deep and dark web forums and collecting information on ways fraud actors are using stolen information to attack the organization.

Fraud risks can be classified in several different ways. The AICPA Forensic and Litigation Services Fraud Task Force has published three Fraud Risk Frameworks (one for business, one for consumers, and one for government aicpa.org/resources/download/fraud-risk-frameworks). Additionally, the ACFE classifies occupational fraud risks into three primary categories: (a) financial statement fraud, (b) asset misappropriation, and (c) corruption. The COSO 2013 IC Framework classifies the types of fraud into three general categories: (a) fraudulent reporting (which includes fraudulent financial reporting, fraudulent non-financial reporting, misappropriation of assets that are **material** to financial reports, and illegal acts), (b) safeguarding of assets, and (c) corruption.

For fraud risk management purposes, this chapter classifies fraud risk types as follows:

- Fraudulent financial reporting
- Fraudulent non-financial reporting
- Misappropriation of assets
- Other illegal acts and corruption

Organizations can tailor these categories to produce an organization-specific fraud risk assessment. In addition, most organizations also consider IT and reputation risk as important parts of their assessments, as discussed below.

Fraudulent Financial Reporting

Any intentional misstatement of accounting information represents fraudulent financial reporting. The types of fraudulent financial reporting typically focus on improving the organization's financial picture by overstating income, understating losses and expenses, or using misleading disclosures. Conversely, some organizations understate income to smooth earnings or avoid taxes.

Each broad category of fraudulent financial reporting includes several potential fraud risks, such as:

- Inappropriately reported revenues, expenses, and balance sheet amounts and inappropriately exaggerated or omitted disclosures
- Concealment of misappropriation of assets, including unauthorized acquisition, disposition, and use of assets
- Concealment of unauthorized receipts and expenditures, e.g., facilitation payments or bribes

Some fraudulent financial reporting fraud risks, e.g., improper revenue recognition, can be achieved via numerous schemes, including backdating agreements, recognizing revenue on product not shipped by period-end, side agreements, or **channel stuffing**. Other fraudulent financial reporting schemes are common across all organizations (e.g., setting aside unsupported reserves for use in future periods and fraudulent **top-side entries/ adjustments**. Some schemes are more industry-specific (e.g., backdating agreements at software companies or manipulating percentage of completion computations for organizations that work on long-term construction projects). Consequently, the fraud risk assessment considers each scheme that could be relevant to the organization.

Organizations can use a fraud risk assessment matrix (see the example shown in Figure 11 at the end of this chapter) to identify and document specific areas of fraud risk and to serve as a foundation for customizing the assessment process for their specific needs. For example, starting with the revenue recognition component of fraudulent financial reporting, the fraud risk assessment considers the following questions:

- What are the main drivers of revenue at the organization?
- Are revenues primarily from volume sales of relatively homogeneous products, or are they driven by a relatively few individual transactions?
- Are revenues recorded automatically or manually?
- Are there any revenue recognition fraud risks specific to the organization's industry?
- What are the incentives and pressures present in the organization (e.g., what personnel receive incentive compensation based on revenue growth)?
- What financial statement metrics do external stakeholders consider to be important?

To address significant marketplace disclosures (e.g., loan delinquency percentages), the following questions are worthy of consideration:

- What controls are in place to monitor internal gathering and reporting of data underlying these disclosures?
- Is there oversight from someone whose compensation is not directly affected by the disclosure?
- Does someone monitor the organization's disclosures in relation to other organizations and ask hard questions about whether the organization's disclosures are adequate or could be improved?

Fraudulent Non-Financial Reporting

Organizations consider the fraud risks that could affect non-financial reporting within their operations. Just as there are common fraudulent financial reporting risks and schemes within industries, there are also common fraudulent non-financial reporting risks and schemes that can lead to:

- Manipulation of environmental, health, and safety records and reports
- Intentional misreporting of key performance indicators and productivity measures
- Falsification of quality-assurance reports
- Falsification of customer metrics or other operational metrics
- Intentional misreporting of Environmental, Social, and Governance (ESG) goals and metrics

When unattainable goals are set, management and other employees may fear the repercussions of not meeting these goals.

Some examples of such fraudulent non-financial reporting include manipulation of safety records that might involve personnel, such as refiners and pipeline operators who maintain detailed safety and repair information, to ensure the optimal and safe operation of their equipment. If personnel perceive excessive budget or time pressure, they may intentionally misreport their labor, e.g., reporting that repairs were made when, in fact, they were not. Similarly, employees and senior management in governmental organizations may feel pressure to misreport program results and outcomes to ensure continued funding at what they consider adequate levels.

Also, intentional false reporting of quality-control metrics can occur when organizations that produce products for the public or other manufacturers have quality control standards with which the organization must comply. Employees may perceive pressure to make timely deliveries of poor-quality products or to avoid the cost of reworking defective products.

Another example is false reporting of educational and professional credentials. Individuals employed by organizations that require certain professional credentials may falsify credentials in order to be hired or retained by the organization. The subsequent discovery of fraudulent credentials can produce reputational and financial damage to organizations.

Assessing and addressing the risk of fraudulent non-financial reporting can be more difficult than addressing fraudulent financial reporting. There is an accepted framework for financial reporting (double entry accounting and generally accepted accounting principles) and checks and balances built within standard accounting processes and controls. However, there may not be an established framework for processing non-financial data and no generalized listing of controls over non-financial data and reports in some industries. Thus, each organization develops its own protocols and controls over the processing of non-financial data relevant to their operations.

Organizations have an inventory of the key non-financial reports on which management relies. Key reports and information are assessed for the risk of fraud in the same manner in which financial reports are assessed. Specifically, organizations consider the incentives and pressures related to the reports, the opportunities personnel have to fraudulently manipulate data, and how the individuals could rationalize their actions.

An organization assessing fraudulent non-financial reporting considers the following questions:

- What are the key reports on which the organization relies to operate effectively?
- What are the key reports or certifications the organization is required to provide by law, rule, regulation, or contractual requirements?
- Is the data contained within those reports from controlled sources, or is it subject to manual intervention and bias?
- Are there non-financial metrics that are important to the organization's stakeholders, including regulators?
- Are there non-financial reports or metrics that can have a direct or indirect impact on personnel compensation or bonuses?
- Who can manipulate or affect these reports or metrics and what controls are in place to prevent the reports and metrics from being altered?
- Are there industry-specific issues the organization needs to consider?

Misappropriation of Assets

Misappropriation of assets by employees, customers, or vendors, criminal organizations, or others affects the following assets:

- Tangible assets, such as cash, inventory, or equipment
- Intangible assets, such as proprietary or confidential product or customer information (such as customer lists or **trade secrets**), protected national security information, personal identifying information (such as Social Security numbers), or credit card numbers
- Proprietary business opportunities

The organization ensures that controls are in place to protect tangible and intangible assets and proprietary business opportunities. Considerations in the fraud risk assessment process include gaining an understanding of what assets are subject to misappropriation, the locations where the assets are maintained, and which personnel have control over or access to tangible or intangible assets.

Common misappropriation schemes are committed by:

- Employees, who might engage in
  - Creation of, and payments to, fictitious vendors
  - Payment of inflated or fictitious invoices
  - Preparation of invoices for goods not received or services not performed
  - Theft of inventory or use of business assets for personal gain
  - Preparation of false or inflated expense claims
  - Theft or use of customer lists and proprietary information
- Employees, who might engage in collusion with vendors, customers, or third parties and
  - Pay for inflated or fictitious invoices
  - Issue inflated or fictitious credit notes
  - Pay invoices for goods not received or services not performed
  - Provide unauthorized preferred pricing or delivery
  - Rig contract bids
  - Engage in theft or use of customer lists and proprietary information
- Vendors, who might create
  - Inflated or fictitious invoices
  - Short shipments or substitution of lower quality goods
  - Invoices for goods not received or services not performed
  - Theft of product in the supply chain
- Customers, who might
  - Make false claims for damaged or returned goods or short shipments
  - Engage in shoplifting
  - Use fraudulent credit cards

- Individuals or groups, who might
  - Make fraudulent claims for government benefits
  - Make fraudulent claims for reimbursements by Medicare or Medicaid
  - File fraudulent tax returns
- Computer hackers, who might steal sensitive information
- Unknown third parties, e.g., cyber-hackers of unknown affiliation

Protecting against these risks requires not only preventive physical and technology-supported analytical safeguarding controls, but also detective controls, such as periodic physical counts of inventory with reconciliations to the general ledger, and the use of data-mining tools. A smart perpetrator may be aware of such controls and design a fraud to circumvent or be concealed from those controls. Personnel conducting the risk assessment keep this risk in mind when considering misappropriation of asset schemes and their effects on the organization.

Know Your Vendors

Any organization that buys goods or services can be victimized by a multitude of vendor and procurement frauds. Consequently, organizations need control activities focused on preventing or early detecting vendor-related frauds. These controls can include:

- Mandating use of competitive procurements
- Careful vetting and credentialing of both new and existing vendors. This includes ensuring they are not on sanction lists, FEIN's have been verified, officers are not criminals, and no conflicts of interests or undisclosed relationships exists
- Enforcing a policy of only doing business with approved vendors
- Closely controlling access to and monitoring of the approved vendor data-base
- Enforcing a policy of non-fraternization between employees and vendors

Fraud risk assessments consider various vendor and procurement fraud schemes (see Fraud Risk Exposures, Appendix F). For each scheme, the risk assessment team will focus on controls such as the above and assess (a) whether the controls are in place and working as intended and (b) whether the controls are sufficient to prevent or detect the relevant scheme. For any residual fraud risks identified, the risk assessment team will consider and apply additional control activities, such as:

- Ensuring that the competitive bidding process is in place and being adhered to
- Requiring frequent rotation of vendors and purchasing and procurement personnel assignments so that inappropriate employee-vendor relationships are difficult to establish
- Using automated vendor credentialing software tools to vet vendors to identify undisclosed relationships and overlapping or interconnected ownerships
- Using data analysis software to compare fields in the vendor data-base with fields in the employee data-base to find matching addresses, phone numbers, bank routing information, or other indications of employee relationships with vendors, including employee-created or employee-controlled vendors
- Employing covert data analytic tests to identify any unusual changes in prices paid, quantities ordered, or delivery addresses
- Using periodic disbursement analyses to review which vendors are being paid and the corresponding amounts
- Looking for anomalies in vendors billing and payment patterns, such as sequential invoicing and rounded total payments to a particular vendor

Control activities for preventing or detecting vendor fraud do not need to be resource-intensive. Simply including a statement such as the following on purchase orders and contracts can serve as a strong deterrent.

> [ABC Corp/Agency] is committed to fair and open competition. If any employee or agent of [ABC Corp/Agency] asks for or solicits anything of value in connection with this purchase order/contract, or if you suspect any impropriety regarding this purchase order/contract, please report this immediately and confidentially to our Director of Compliance and Risk Management, Jane Honest, at 555.555.5555 or at J.Honest@abccorp.com.

Other Illegal Acts and Corruption

Fraud risk assessments also include consideration of illegal acts, including actual or suspected noncompliance with laws and regulations and other corrupt behaviors. These can include matters that have a direct effect on financial statements and other laws, regulations and matters that may be fundamental to business operations or may involve material penalties. Corruption can include a wide variety of misuses of entrusted power for private gain.

These risks may include:

- Violations of anti-bribery regulations, including payment or receipt of bribes and improper gratuities by companies, private individuals, and public officials
- Bid-rigging or other manipulation of purchasing activities for private gain
- Violation of the U.S. **False Claims Act** or other relevant national or local laws or regulations
- Failure to comply with banking and financial services regulations, including the U.S. Bank Secrecy Act, and anti-money laundering and anti-terrorist financing requirements
- Compliance with regulations relating to securities market manipulation and **insider trading**
- Violations of data protection laws, including theft and illicit use of personal and other sensitive information, such as government identification and bank account numbers, trade secrets, and national security information
- Compliance with tax and pension obligations and payments
- Violations of labor, technology export, or consumer protection laws, such as price fixing, human trafficking, or willful sale of unsafe products
- Violations of environmental protection, public health, and safety laws
- Industry-specific laws and regulations, such as those pertaining to the healthcare industry or government contractors

Anti-bribery regulations have global reach. In the United States, for example, the FCPA prohibits U.S. entities, their foreign subsidiaries, and others from bribing foreign government officials, either directly or indirectly, to obtain or retain business.[7] There are similar anti-corruption laws in the United Kingdom (Bribery Act 2010) and other countries, as well as guidelines established by the United Nations Convention Against Corruption, to which many countries are either signatories or parties.

Organizations that have operations outside their home country may leverage additional resources. Transparency International is a non-profit, non-governmental, multinational organization focused on anti-corruption and transparency in business and government. The **Corruption Perceptions Index** (CPI), annually ranks countries and territories based on their perceived levels of corruption. The CPI can assist organizations in prioritizing their anti-corruption efforts in areas of the world where their operations are at greatest risk as well as in the organization's home country.

Another form of corruption is aiding and abetting. Law enforcement authorities worldwide have prosecuted numerous cases in which organizations were knowingly structuring transactions or making representations that enabled other organizations to fraudulently misstate their financial statements. A thorough risk assessment considers the risk that someone may be engaging in such behavior as well as other types of corruption that may be applicable to the organization.

Regulatory and legal misconduct includes a wide range of risks, such as conflicts of interest, insider trading, theft of competitor trade secrets, **anti-competitive practices,** environmental violations, and trade and customs regulations in areas of import/export. Depending on the particular organization and the nature of its business, some or all of these risks may be applicable and, therefore, are considered in the risk assessment process.

Reputation Risk

Reputation risk is evaluated differently by organizations, either as a separate risk or the end result of other risks (e.g., operational, regulatory, or financial reporting). Fraudulent acts can damage an organization's reputation with customers, suppliers, other stakeholders, the public in general, and the capital markets.

For example, fraud leading to a **financial restatement** damages an organization's reputation in the capital markets, which could increase the organization's cost of borrowing and depress its **market capitalization**. In government, reports of fraud diminish public confidence, which can bring a confluence of adverse impacts. Because the board is responsible for the longevity of the organization and has responsibilities to multiple stakeholders, it will evaluate its performance regularly with respect to reputation risks and ensure that consideration of reputation risk is part of the organization's risk assessment process.

Information Technology Cybersecurity and Fraud Risk

Organizations rely on IT to conduct business, communicate, and process information. Many consider cyber risks the #1 national security risk. Cyber risk has been on the U.S. Government Accountability Office's high-risk list since 1997.

[7] The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. [See justice.gov/criminal-fraud/foreign-corrupt-practices-act.].

A poorly designed or inadequately controlled IT environment can expose an organization to internal and external fraud.

Computer systems linked by national and global networks face an ongoing threat of cyber fraud and a variety of threats that can result in significant financial and information losses. Information technology risks include threats to data integrity, threats from hackers to system security, and theft of financial and sensitive business or personal information.

Whether in the form of hacking, economic espionage, denial of service attacks, web site defacement, sabotage of data, viruses, or unauthorized access to data, IT fraud risks can affect everyone. Information included in *COSO in the Cyber Age* can provide organizations with relevant information about the ever-changing cyber risks organizations face.

People who intend to commit fraud can use IT in any of the fraud risk categories. Examples of those risks by category include:

- **Fraudulent financial reporting**
  - Unauthorized access to accounting applications — Personnel with inappropriate access to the general ledger, subsystems, or the financial reporting tool can post fraudulent entries.
  - Override of system controls — General computer controls include restricted system access, restricted application access, and program change controls. Information technology personnel may be able to access restricted data or adjust records fraudulently.
- **Fraudulent non-financial reporting**
  - Intentional false reporting of health and safety metrics — Organizations that operate in heavy manufacturing industries or natural resource extraction industries normally have established health and safety guidelines that are supported by measurement and reporting mechanisms. Individuals may perceive pressure to provide the appearance that the operation is meeting standards or to avoid the cost of necessary repairs and maintenance that would be required to improve the metrics. Individuals may have access to key reports within the IT system and may change data to commit the fraud.
  - Intentional false reporting of key performance indicators and business metrics — In many industries, business metrics or performance indicators are important for management decision-making. Some, like contract bookings or operating metrics, may be publicly reported to investors. Sources of information for such metrics are considered and governed by the organization's anti-fraud controls.
  - Intentional false reporting on Environmental, Social and Governance (ESG) and sustainability initiatives and metrics — Investors increasingly focus on ESG and sustainability reporting to assess financial risks due to these factors. False, unrealistic, or deliberately misleading ESG reporting can result in costly litigation and financial and reputational damage. For more on ESG and fraud, see *Managing Fraud Risks in an Evolving ESG Environment* by ACFE and Grant Thornton.
- **Misappropriation of assets**
  - Theft of tangible assets — Individuals who have access to tangible assets (e.g., cash, inventory, and fixed assets) and to the accounting systems that track and record activity related to those assets can use IT to conceal their theft of assets. For example, an individual may establish a fictitious vendor in the vendor master file to facilitate the payment of false invoices, or someone may steal inventory and charge the cost of sales account for the stolen items, thus removing the asset from the balance sheet.
  - Theft of intangible assets — Given the transition to a services-based, knowledge economy, intangible assets are increasing in value, e.g., customer lists, business practices, patents, and copyrighted material. Examples of theft of intangible assets include piracy of software or other copyrighted material by individuals either inside or outside of the organization.
- **Other Illegal acts and corruption**
  - Misuse of employee or customer data — Personnel within or outside the organization can obtain employee or customer data and use such information to obtain credit or to commit other frauds.
  - Theft of confidential data — Confidential data theft continues to be a risk to all organizations. Ransomware attacks (where the organization's data is encrypted and held hostage), cyber-attacks by foreign governments, and theft of PII (personally identifiable information) by employees and computer hackers are just some of the threats governments and the private sector face every day.

Cyber fraud perpetrators do not even have to leave their homes to commit fraud, as they can route communications through internet service providers and wireless and satellite networks. They may go through computers located in several countries before attacking targeted systems around the globe. Any information — not just financial information — is at risk, and the stakes are very high and rising as technology continues to evolve.

To manage the ever-growing risks of operating in the information age, it is important for an organization to know its vulnerabilities and be able to mitigate risk in a cost-effective manner. Therefore, IT risk is incorporated into an organization's overall fraud risk assessment.

Blockchain Asset Considerations

Adoption of digital assets is emerging across not just financial institutions, but also the manufacturing, logistics, retail, commodities, and global trade sectors. Organizations are cautioned to understand digital-asset risk exposures inside their businesses, across value chains, and with third-party partners.

Digital assets (cryptocurrency or virtual currency) and their underlying blockchain technology provide the capability to tokenize any asset or medium of value. Everything from real estate to intellectual property to sneakers to money can be tokenized. Tokenization enables faster and cheaper transactions through automation and smart contracts, providing (potentially) more transparency and accessibility.

Non-Fungible Tokens

A popular form of tokenization, known as non-fungible tokens or NFTs, are unique items verified and secured by a blockchain, the same technology used for cryptocurrencies. An NFT provides information around authenticity, ownership and uniqueness of the item. Digital collectables that have been tokenized such as artwork, digital sports trading cards, media clips, and even digital real-estate, are considered NFTs.

Digital assets are not immune to fraud risks. The rapidly evolving nature of the digital-asset ecosystem warrants strong compliance, legal, and consumer protection controls. In the context of assessing fraud risk, the following considerations are important:

- Prior to any strategic pivot to a digital asset-based model or incorporation of cryptocurrencies for payment facilitation, fraud risks warrant careful and specific consideration.

- Committing appropriate resources with sufficient digital asset-specific experience and qualifications is key in implementing and monitoring fraud-related control activities.

- Organizations need to understand both the common and unique fraud-related risks digital assets present. In October 2018, the National Institute of Standards and Technology published NISTIR 8202: Blockchain Technology Overview that may be synchronized with any organization's technical evaluation of blockchain-related fraud risks. Such risks include:
  - Technical stability and structure: Is the blockchain permissioned? Does it employ proof-of-work, proof-of-stake, or some other consensus mechanism? What is the node-diversity of the blockchain? How are we securing and granting access to keys or signatures?
  - Digital-asset utility: Does the utility of the digital asset sufficiently reduce fraud risks? Is the specific digital asset appropriate to the use case as an exchange of value or information?
  - Auditability: How does the blockchain enable auditing the value chain and financial information? How transparent and accessible will that be within the organization?
  - Hacking and theft: How secure is the network and who controls it? Is it vulnerable to coordinated attack or excessive downtime?
  - Cyber attacks: How do we mitigate the risk of malicious users both internally and externally? How do we address altered chains, spoofing, and diversion (theft)?
  - Resource usage: Is the blockchain resource-intensive, requiring excessive participants and potentially more oversight.
  - Financial reporting: How will tokenization affect the ability to appropriately report business income, financial health, and asset values?

- Digital-asset control activities related to internal fraud, consumer protection, and retail payment mechanisms will specifically address:
  - Compromised user credentials (internal and external)
  - Recoverability of fraudulent digital-asset payments
  - Traditional fraud schemes including counterfeiting, elder fraud, Ponzi and pyramid schemes, and identity theft
  - Unauthorized cryptographic changes and forks
  - Altered underlying smart-contract terms
  - Use of material non-public information depending on the transparency and accessibility of the blockchain used
  - Risks related to system degradation or downtime

- Even if not utilizing digital assets themselves, assessing secondary exposure to digital-asset risks will be included in product, customer, service provider, and vendor assessments.

Understanding digital-asset technology and how it affects the organization is important and is indeed representative of fraud risk management challenges; however, the fundamentals of combatting fraud remain the same. For more information on digital-asset considerations, see *Blockchain and Internal Control — The COSO Perspective*.

Specifically Considers the Risk of Management Override of Controls

An important part of the fraud risk identification process involves specific consideration of the potential for wrongdoing by management and the risk of management override of internal controls, including the controls that are established to prevent or detect fraud.

Fraud and wrongdoing perpetrated by the board and management are among the most damaging to organizations, because the trust and authority given provides greater opportunity for fraud. Leaders can also direct others to wittingly or unwittingly participate in improper conduct.

Members of management sometimes use their knowledge of the organization's controls to conceal their actions. For example, a manager who has the authority to approve new vendors may create and approve a fictitious vendor and then submit invoices for payment, rather than only submitting false invoices for payment. Members of management can also abuse their organizational influence to stifle attempts to report wrongdoing.

Employees may find it difficult to raise the risk of management override or wrongdoing during a fraud risk assessment because of the appearance of criticizing a superior in the organization. Making such risks a standard part of any fraud risk assessment can help diffuse such tension.

It is also important to keep the risk of management override of controls in mind when evaluating the effectiveness of controls. A fraud risk management control is not effective if it can be overridden easily. (See Chapter 3, which includes additional information on considering management's ability to override controls, and *Management Override of Internal Control: The Achilles' Heel of Fraud Prevention*.)

Assesses the Likelihood and Significance of Risks Identified

The fraud risk assessment team analyzes identified risks through a process that includes estimating the potential likelihood of the fraud occurring as well as the potential significance of the fraud if it occurs. The risk assessment team carefully evaluates the likelihood and significance of identified fraud risks based on historical information, known fraud schemes, and interviews with business-process owners.

Assessing the likelihood and significance of each potential fraud risk is a subjective process. All fraud risks are not equally likely, nor will all frauds have a significant effect on every organization. Also, assessing the likelihood and significance of identified **inherent risks** allows the organization to manage its fraud risks and apply preventive and detective procedures rationally.

It is important to first consider fraud risks to the organization on an inherent basis, i.e., without consideration of known controls. This approach allows management to consider all relevant fraud risks and then to design controls to address those risks.

Likelihood

Management's assessment of the likelihood of a fraud risk occurring is informed by instances of that particular fraud's occurrence in the past at the organization, the prevalence of the fraud risk in the organization's industry, and other factors. Those factors include the number of individual transactions, the complexity of the risk, the number of people involved in reviewing or approving the process, and the results of past audits.

Inherent vs. Residual Risk

Inherent risk is the amount of risk that exists absent control activities. With no controls in place, a warehouse of gold bullion has a high degree of inherent risk. A warehouse of topsoil, has a relatively lower degree of inherent risk.

A specific fraud vulnerability with high degrees of both likelihood and significance, therefore, has high inherent risk. It warrants more fraud controls.

Residual risk is the amount of risk that remains after control activities are successfully implemented. These include both the inherent risks that are either not controlled, or are controlled but the control activities are defeated or rendered ineffective.

For example, if an organization periodically conducts a random inventory audit, an item outside the sample set could still be misappropriated, which would represent residual risk. Likewise, fraud actors could subvert this **control activity** if they were to gain foreknowledge of the audit or collude with a third party to falsify inventory records.

By assessing the likelihood and significance of both inherent and residual risks, an organization can gain a better understanding of its vulnerability to a particular fraud scheme. When no residual risk can be identified, additional fraud control activities are not considered. When residual risk is identified, additional fraud control activities are considered.

Organizations categorize the likelihood of potential frauds occurring in as many gradations as deemed reasonable. However, three categories are generally adequate: remote, reasonably possible, and probable.

Significance

Management's assessment of the significance of a fraud risk includes not only the financial statement and monetary significance, but also the significance to an organization's operations, brand value, and reputation, as well as criminal, civil, and regulatory liability. Consider, for example, two different organizations with similar amounts of expenses charged via employee expense reports. One of those organizations is a professional services firm that charges those expenses to clients. Although the likelihood of the risk of fraudulent expense reports and the monetary exposure may be similar at both organizations, the relative significance of fraudulent expense reports to the professional services firm may be greater given the impact that fraudulent expense reports can have on customer and contractual relationships.

Organizations can categorize the significance of potential frauds in as many gradations as deemed reasonable. However, these three categories are generally adequate — inconsequential, more than inconsequential, and material.

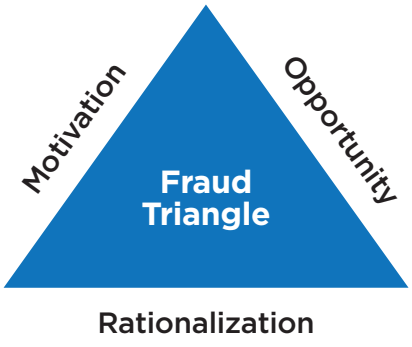
Considers the Fraud Triangle and Other Models to Evaluate the Risk Landscape

A rigorous fraud risk assessment process incorporates the current academic and practitioner research on fraud attributes and characteristics. Risk assessments frequently reference and consider various models of fraud.

One traditional and well-adopted model is the **Fraud Triangle**, developed by Donald Cressey and others starting in the 1950s. This model recognizes that most frauds include three important elements:

- Incentives and pressures that motivate an individual to commit a fraudulent act
- Opportunities or perceived opportunities that provide an individual with some assurance that a fraudulent act can be committed without being detected
- Attitudes or rationalizations that enable an individual to internally justify the performance of a fraudulent act

Figure 6. The Traditional Fraud Triangle



Other researchers and practitioners have expanded or enhanced the Fraud Triangle to include the attributes of Arrogance and Competence. This model is sometimes referred to as the Fraud Pentagon.[8]

Figure 7. The Fraud Pentagon

- Arrogance, or lack of conscience, is an attitude of superiority or entitlement or greed on the part of a person who believes that anti-fraud measures do not personally apply
- Competence is an individual's expertise to execute the scheme; access to assets, people, or systems; an ability to override controls; concealment of wrongdoing; and the ability to control the social situation through rationalization, persuasion, lies, or coercion and to manage the related stress

These models focus primarily on the attributes of potential perpetrators. While the investigation and analysis of identified frauds typically finds the elements and attributes of either the Fraud Triangle or the Fraud Pentagon, they are not perfect predictors. For example, it can be difficult to fully assess individual incentives, motivations, rationalizations, pressures, arrogance, and competence of fellow employees and individuals. The inner thoughts and motivations of individuals are often revealed by their actions, but no organizational assessment can presume to know them all. Also, these attributes may be readily observed among employees, managers, and business leaders who are not perpetrators, blunting their usefulness in assessing risk.

[8] See Improving fraud risk management with an enhanced Fraud Triangle; Boyle, DeZoot, Hermanson, and Wolfe; *ACFE Fraud Magazine*, March/April 2018. See also, *Fraud Pentagon - Enhancements to the Three Conditions Under Which Fraud May Occur,* by Jonathan T. Marks, CPA, CFE.

Ultimately, the element of the Fraud Triangle over which an organization can exert the most control is opportunity.

Some risk assessments leverage other models that focus on attributes of the underlying schemes or the interaction between risks and controls. For example, the Fraud Triangle of Action model considers three essential elements of a fraudulent scheme, all of which can be addressed through anti-fraud controls.[9]

Recent academic and practitioner researchers have attempted to integrate these models into an Advanced Meta-Model of Fraud.[10]

Figure 8. The Triangle of Fraud Action

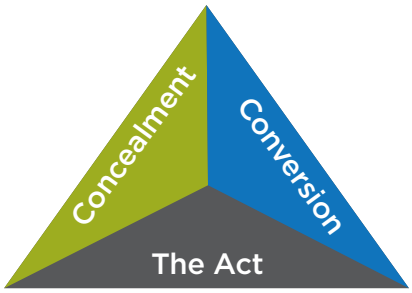
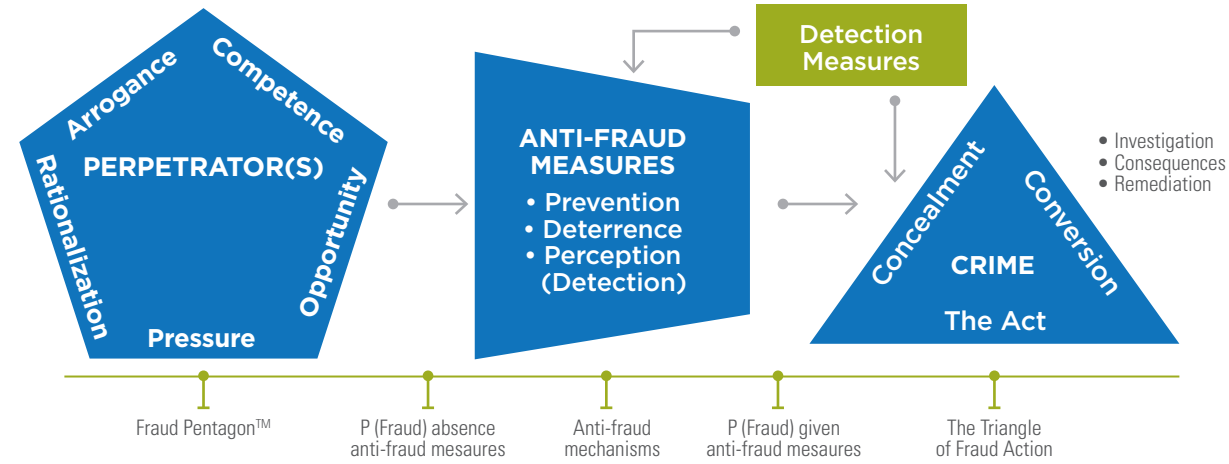


Figure 9. The Advanced Meta-Model of Fraud



Comprehensive risk assessments consider both traditional and current thinking on fraud risks to inform the assessment process. Leveraging one or more of these models to inform the risk assessment allows for fulsome and detailed discussion of potential perpetrators, schemes, and risks.

Incentives and Pressures

The assessment of fraud risk considers the incentives or pressures that might induce a perpetrator to commit fraud. Organizations have a range of incentives in place to motivate employees to achieve objectives. Some individuals may resort to fraud in order to obtain incentive compensation. Pressures, both real and imagined, exist within organizations to achieve their objectives. The fraud risk assessment team gains an understanding of the factors causing pressure to achieve the organization's objectives.

Motives for committing fraud are numerous and diverse. One executive may believe that the organization's business strategy will ultimately be successful, and, if there are interim negative results, decide to conceal them to give the strategy time. Another executive might need just a few more pennies per share of income to qualify for a bonus or to meet analysts' estimates. A third executive might purposefully understate income to save for a rainy day or avoid taxes. The fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud. The board evaluates incentive programs for senior executives and management evaluates these programs for others in the organization. The evaluation addresses how those executives and managers may affect employees' behavior when conducting business or applying professional judgment (e.g., estimating bad debt allowances or revenue recognition).

Incentive compensation and the metrics on which they are based can provide a map to where fraud is most likely to occur. There also may be non-financial incentives, such as an individual who decides to record a fictitious transaction to avoid explaining an otherwise unplanned variance. Even maintaining the status quo is sometimes a powerful enough incentive for personnel to commit fraud. Personnel at an operating unit or location vulnerable to closure may collude to misstate operating results to avoid closure and keep their jobs.

[9] Mary-Jo Kranacher and Richard Riley, *Forensic Accounting and Fraud Examination,* 2nd Edition, John Wiley & Sons, p. 24.

[10] Richard Riley, Scott Flemming, and Jonathan T. Marks, Meta-model of fraud, *ACFE Fraud Magazine,* July/August 2018. See also *(Advanced) Meta-model of Fraud - Two triangles combine for better fraud case comprehension*, by Jonathan T. Marks, CPA, CFE.

Also important and often harder to recognize are the pressures on individuals to achieve performance or other targets. Some organizations are transparent, setting specific targets and metrics by which personnel will be measured. Other organizations are more indirect and subtle, relying on the corporate culture to influence behavior.

Although individuals may not have any incremental monetary incentive to fraudulently adjust a transaction, for example, there may be ample pressure on an employee, either real or perceived, to act fraudulently.

Data analytics can identify management practices and business processes that encourage employees to bypass controls and can highlight risk factors that could identify rogue behavior, excessive spending, or other anomalies.

Pressure to Meet Aggressive Goals

One of the most underrated fraud risk drivers is the pressure for staff to meet aggressive goals set by management. One high-profile example is the Wells Fargo Fake Account Scandal. From 2002–2016, managers at Wells Fargo Bank applied pressure on branch employees, encouraging them to market and sell different financial products and services, such as bank accounts, credit cards, and so forth. The sales goals became unachievable and with the job-threatening consequences put in place, employees began signing customers up for services they did not need and opening accounts for clients without their knowledge or permission. When the extensive fraud finally came to light, Wells Fargo agreed to pay a $3 billion settlement.[11]

Attitudes and Rationalizations

The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions. Attitudes about fraud and rationalizations for committing fraud are characteristics of individual employees, vendors, customers, and others outside of the organization. Therefore, they vary by individual. An organization can influence, but not completely control, the attitudes of its employees through its hiring and evaluation processes and in the tone established by leadership and senior management. An organization can exercise some control over its vendors through the criteria included in the vendor selection process, ongoing monitoring of its activities with vendors, and ensuring that vendors understand that fraud will not be tolerated. Government can exercise some control over members of the public who may fraudulently claim benefits through leading-edge data analytic and other prevention controls before a payment is made and rigorous prosecution when fraud is uncovered.

Rationalizations for committing fraud vary by individual and thus are outside an organization's control. For example, one person might rationalize a fraud act by comparing it to an even more egregious act that he or she did not commit ("I only stole $10,000 and I could have stolen much more") or by justifying the action in relation to his or her personal life ("I did it to provide for my family").

Data analytics can be an effective fraud deterrent. If people know that overt and covert analytics are being employed, they will be less likely to commit fraud.

Opportunities

The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets; altering of the entity's reporting records; or committing other inappropriate acts. Weak internal controls and poor segregation of duties can provide opportunities to those who wish to commit fraud.

Opportunities to commit fraud exist throughout organizations and may be reason enough to commit fraud. These opportunities are greatest in areas with weak internal controls and a lack of segregation of duties. However, some frauds, especially those committed by management, may be more difficult to detect because management often can override internal controls. Therefore, appropriate monitoring of senior management by a strong board and audit committee, supported by internal auditing, is critical to fraud risk management. In addition, fraud by external parties, such as a criminal ring posing as a physician to defraud Medicare and Medicaid, continue to be a problem.

Data analytics can help to prevent the occurrence of fraud by verifying that key controls are in place and working properly.

Identifies Existing Fraud Control Activities and Assesses Their Effectiveness

Organizations usually have existing controls in place that can serve as preventive or detective fraud control activities. As part of the fraud risk assessment process, the risk assessment team examines each specific fraud scheme or risk and identifies the relevant existing preventive and detective control activities.

[11] See Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts without Customer Authorization.

For some fraud schemes, there may be several existing controls. For other fraud schemes, the risk assessment team may conclude that no controls exist. After identifying existing control activities, the risk assessment team evaluates how effective these existing fraud control activities are in terms of mitigating fraud risk.

This control effectiveness assessment process requires two steps. First, a determination will be made as to whether the control is in place and functioning as designed. Once that determination is made, the control will be reassessed in terms of its effectiveness for preventing and detecting fraud.

This first step will be relatively straightforward for organizations that have implemented the COSO *Internal Control — Integrated Framework*. Under the COSO Framework's Monitoring Component, the organization will know, through regular control testing, whether a particular control is in place and working as designed. (An organization that has not implemented the COSO Framework will need to test the controls to complete the first step.)

If an organization only focused on accuracy in accounting and financial reporting when it designed its internal controls, their effectiveness in terms of fraud prevention and detection may be inadequate.

In designing internal control processes and procedures, organizations often start with accounting processes and cycles and design controls accordingly. Fraud risk management, however, follows a fraud-scheme-specific approach:

- Identify all possible fraud schemes (not just those related to accounting and financial reporting)
- Assess the existence and effectiveness of controls that would prevent or detect those schemes
- Design and implement additional, fraud-focused control activities in order to address residual fraud risk

Some examples will help illustrate how internal control and fraud risk management intersect and support each other.

- **Segregation of Duties —** Duties segregation is a standard (and usually effective) control procedure that is designed to prevent a single individual from controlling all transaction steps. In a fraud risk assessment, this control would likely be identified as an existing control when looking at employee embezzlement fraud schemes. In specific circumstances, the fraud risk assessment team might conclude that its effectiveness is limited from a fraud risk perspective, because the employees across which duties are segregated could collude to override that control. The fraud risk assessment team might then conclude that the residual fraud risk (that employees might collude) needs to be addressed by adding an additional control, such as implementing a policy of periodically rotating new employees into the duties so that chances of collusion are reduced.

- **Approved Vendor Lists —** Many organizations have a control in place that prevents doing business with any organization that has not been vetted and placed in the approved vendor data-base. In a fraud risk assessment, this control would likely be identified as an existing control when looking at purchasing fraud schemes. In specific circumstances, the fraud risk assessment team might conclude that its effectiveness is limited from a fraud risk perspective (e.g., an employee with access to the data-base can add a phony vendor and then direct payments to that vendor). The fraud risk assessment team might then conclude that the residual fraud risk (that an employee might add a phony vendor) needs to be addressed by adding an additional control, such as periodically using data analytics to compare all fields in the employee data-base and the approved vendor data-base. (Such an additional **fraud control activity** will be more effective if carried out covertly.)

- **Higher Transaction Approval Authorities —** Most organizations have a control in place that establishes thresholds for approval of transactions — particularly purchasing transactions — by higher levels of management or by more senior personnel. In a fraud risk assessment, this control would likely be identified as an existing control when looking at purchasing fraud schemes. In specific circumstances, the fraud risk assessment team might conclude that its effectiveness is limited from a fraud risk perspective, because employees can split purchases into several smaller transactions to avoid obtaining higher-level approvals. The fraud risk assessment team might then conclude that the residual fraud risk (purchase-splitting) needs to be addressed by adding an additional control, such as performing a Benford's Law analysis of purchase amounts on a regular basis. (Again, such an additional fraud control activity will be more effective if carried out covertly.)

- **Asset Verification Physical Counts —** Requiring periodic physical counts of key assets is a standard control activity designed to assure that assets recorded in the accounting system actually exist. In a fraud risk assessment, this control would likely be identified as an existing control when looking at asset misappropriation fraud schemes. In specific circumstances, the fraud risk assessment team might conclude that its effectiveness is limited from a fraud risk perspective, because assets can be moved during inventory counts or empty boxes

can be disguised to look like they contain assets. The fraud risk assessment team then might conclude that the residual fraud risk (altered or stolen inventory) needs to be addressed by adding additional controls, such as performing surprise inventory counts, performing simultaneous counts at all inventory locations, and changing the actual counting process and procedures.

The extent to which existing internal control processes and procedures might be adequate to address fraud risk is a function of whether or not those controls were designed with possible fraud foremost in mind. Additionally, even if existing controls were designed with possible fraud in mind, the reality is that if such controls focused primarily on accuracy in accounting and financial reporting, those controls might not consider the wider range of fraud schemes to which an organization might be vulnerable.

After assessing the effectiveness of these existing controls, certain residual risks remain, including the risk of management's override of established controls. The risk assessment team evaluates the potential of those residual risks and determines the nature and extent of the fraud preventive and detective controls and procedures required to address such risks. The fraud risks that were deemed to be highly likely and highly significant are a priority. In addition, an organization also considers the array of other risks not deemed to be highly likely and highly significant.

Thus, the final step in the risk assessment process is to determine whether any residual fraud risk exists and whether any existing residual fraud risk needs to be addressed through an appropriate response. The risk assessment team also begins to evaluate controls optimization, noting instances of apparently unnecessary or redundant control activities to mitigate a single risk. The existence of too many controls can serve to introduce fraud risk if systems become so cumbersome that personnel lose sight of key controls in the maze of seemingly unnecessary control activities.

Determines How to Respond to Risks

Risk assessment includes considering how the risk is managed and whether to accept, avoid, reduce, or share the risk.

Risk tolerance varies from organization to organization. At the highest level, the board sets the organization's risk tolerance, taking into consideration its responsibilities to all shareholders/citizens, capital providers, and other stakeholders. While some organizations want only to address fraud risks that could have a material financial statement impact, other organizations want to have a more robust fraud response program. For example, some organizations consider a zero-tolerance policy for corruption and money-laundering an important factor in meeting governance objectives for enterprise risk. In addition, a desire for a more robust fraud response is generally the case in government, where mission and program achievement and safeguarding public assets are paramount.

Many organizations state that there is a "zero-tolerance" policy with respect to fraud. However, fraud deterrence almost always carries a cost, and often organizations compare the costs of controls to the likely impacts, both financial and non-financial, and make the determination that certain fraud risks are too expensive and time-consuming to address via controls. Consequently, the organization may decide not to put control activities in place to address such risks or to put only detective control activities in place rather than spend resources on preventive control activities. This would be considered "accepting" the fraud risk.

An organization's risk tolerance provides management with support about how to respond to fraud risk. Fraud risks are addressed by accepting the risk of a fraud based on the perceived level of likelihood and significance, increasing the controls over the area to mitigate the risk, transferring the risk through a third party such as an insurance policy, or terminating the activity or objective with which the risk is associated.

The board ensures that management has implemented the right level of controls based on the risk tolerance it has established for the organization. In effect, the organization looks at its financial statements, programs, and operations and asks, "What can be wrong in this picture?" Then, management designs appropriate control activities. The key is to be selective and efficient.

Many potential controls could be put in place. The goal is a targeted and structured approach rather than an unstructured or haphazard approach. In addition, it is important to include efficient controls that deliver the most benefit for the cost of resources.

In addressing fraud risks, the organization is careful to ensure that fraud risk management controls are designed appropriately to address the relevant risks and that those controls also are operating effectively and efficiently. In those situations in which an internal control might be executed with limited skepticism (e.g., agreeing an accrual balance to underlying support), a fraud risk management control includes an evaluation of the underlying support

for consistency in application from prior periods and for potential inappropriate bias. Therefore, the design of the fraud risk management controls is appropriate and is executed by competent and objective individuals.

Management's documentation of fraud control activities includes the description of what the control is designed to do, who is to perform the control, who is to monitor and assess the effectiveness of the control, and the related segregation of duties. (The section "Integrates with the Fraud Risk Assessment" in Chapter 3 discusses the linkage of the fraud risk assessment to fraud controls.)

Uses Data Analytics Techniques for Fraud Risk Assessment and Fraud Risk Responses

Data analytics are vital tools in evaluating the effectiveness of organizational control activities. Traditionally, evaluating controls was performed manually with assistance in varying degrees from automation, mostly with spreadsheets and basic rules-based analytics. Rules-based analytics examine a limited number of data sets via a simple Boolean condition (i.e., a value that is either true or false or that can be answered with yes or no). Today, with sophisticated data analytics techniques, like those identified in this chapter and in Appendix D, it is possible to identify control activities' strengths and weaknesses, not just more effectively, but also across greater sectors of an organization on a more proactive basis to better assess, not just detect, fraud risks.

When considering what data elements could be most helpful in a risk assessment, it is best to start by asking the right fraud risk questions first, as in the context of the Fraud Triangle, then map the data sources to those fraud risk opportunities. For example, if fraud risks are primarily related to sales, customers, or distributors, then looking at order-to-cash and sales data is often the best place to start. If the risks are related to theft of assets, either physical or digital, then looking at employee access controls may be best. If the top risks are related to cash disbursements to third parties, then an examination of the procure-to-pay, vendor-payment process could be most relevant. To evaluate the effectiveness of controls to ensure honest, fair, impartial, and legal contracting (i.e., procurement integrity), data analytics techniques can identify red flags such as the following that indicate control activity weaknesses:

- A pattern of awards followed by change orders that increase the prices of the contracts
- Excessive sales discounts, returns, or their relative timing with respect to period cut-offs
- Invoices significantly higher than the average cost of similar services/goods
- Disparity in bid prices greater than a threshold value
- Existing financial relationships between vendors and the procuring entity's employees
- Suspicious keyword terms or descriptions in sales or payment data, specifically in the comments field of a transaction
- Prices dropping when a new or infrequent competitor enters a competition; patterns of anti-competitive cost submissions in bids; invoicing inconsistent with contract terms
- Vendors and procurement professionals with identical personal information (i.e., emails, bank accounts, addresses, telephone numbers)
- Percentage of sole-source contract awards

Data analytics techniques can also help isolate transactions or trends that represent potential fraud.

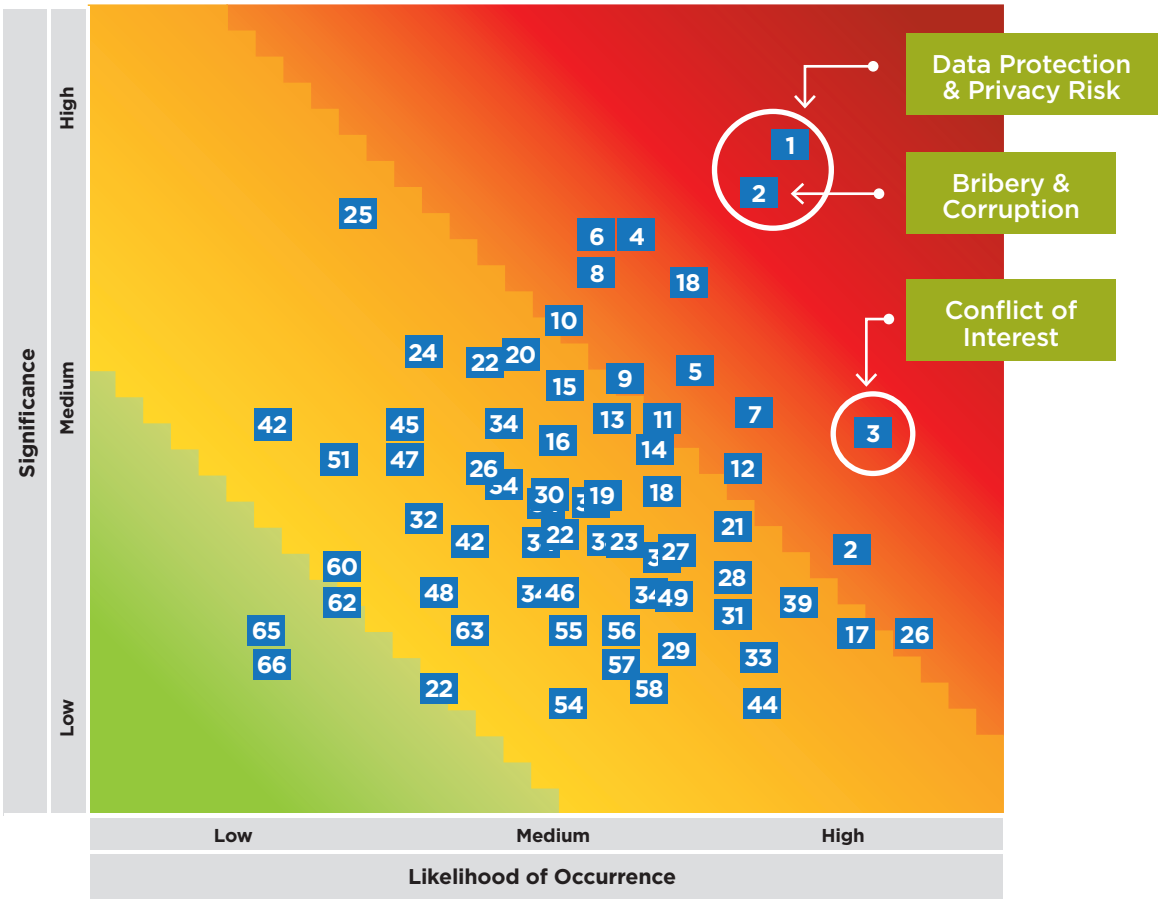
Organizations can utilize some of the concepts included in auditing standards in their application of data analytics in the fraud risk assessment.[12] Professional guidance requires the external audit practitioner to perform disaggregated analytics on revenue as part of the fraud risk assessment process. That guidance also encourages the external audit practitioner to devise appropriate data analysis strategies for each identified risk.

Data analytics can also be used to represent some of the more relevant risks that an organization faces with various visualization tools. For example, organizations often utilize employee surveys, facilitated sessions, and other data-gathering techniques to gain a more reflective perspective on fraud risks. They then use data analytics techniques to compile, display, and analyze the results.

The results of data analytics can, for example, be used as part of the fraud risk assessment process in a **data visualization** of identified fraud risk likelihood and significance in a **heat map** display. The following is a hypothetical example. Different organizations could make different judgments about the significance or likelihood of various types of risks.

[12] AU-C section 240, Consideration of Fraud in a Financial Statement Audit [See aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00240.pdf.]; PCAOB AS 2110, Identifying and Assessing Risks of Material Misstatement [See https://pcaobus.org/oversight/standards/auditing-standards/details/AS2110]; and International Standard on Auditing 240 [See ifac.org/system/files/downloads/a012-2010-iaasb-handbook-isa-240.pdf.] provide guidance to external auditors regarding fraud risk assessment and response.

Figure 10. Fraud Risk Assessment Heat Map



Data analytics techniques, ranging from simple categorization and stratification to sophisticated predictive and prescriptive models, can assist organizations in focusing their fraud risk responses on the areas in which fraud is a higher risk. Some data analysis techniques to gather fraud risk evidence include:

- **Data stratification** — Sorting or categorizing payments, third parties, survey data, employee information, journal entries, and other sources by account type, over time, by dollar amount, or by some other logical grouping can help identify outliers and anomalies. For example, sorting on a key field can quickly identify items that do not follow the organization's numbering or labeling standards.

- **Risk scoring** — Assigning weights to various fraud risks on an objective and repeatable basis can help surface the risk areas on which to focus.

- **Trend analysis** — Analyses of trends over time or across locations can be helpful in identifying outliers that may indicate the existence of fraud or error. Particularly helpful in identifying fraud are trend analyses of ratios that compare financial data to operations data. Individuals who are intent on committing fraud may only have the ability to manipulate financial amounts or operational data, but not both. Examining meaningful disaggregated ratios of financial data to operational data can identify outliers or trends that can be investigated for potential fraud. For example, a monthly trend analysis of revenue per case of product sold is assessed. If there is a month in which the revenue per case sold is significantly higher than it is in other months, this could be an indication of an erroneous or fraudulent journal entry. If the revenue per case sold is significantly lower, this could be an indication of poor pricing, billing errors, or fraud.

- **Fluctuation analytics** — Comparing current year to previous year statistics can highlight unusual trends or anomalies (e.g., activity against a dormant account).

- **Data visualization** — When viewing such data, anomalies

and patterns are far more likely to be spotted when visualized in a graphical chart, heat map, or dashboard compared to being displayed in a spreadsheet by rows and columns.

- **Statistical analysis/predictive modeling** — For organizations deploying continuous monitoring, this data can provide valuable perspectives on emerging fraud risks or predictive models, e.g., taking lessons learned from past events to identify or predict future high-risk areas in the organization.

- **Using information from external data sources** — In analytics this would include news and media articles of emerging fraud risks, industry events, and regulatory actions as well as index data, such as the CPI, among other sources or industry-specific publications.

In summary, when performing a comprehensive fraud risk assessment, data analytics can be more efficient in identifying potential fraud risks across a broader sector of an organization; providing tangible evidence of control activity strengths and weaknesses; and assisting in organizing, prioritizing, and visualizing those fraud risks needing greater attention.

For more information on the use of data analytics, please refer to Appendix D.

Documents the Risk Assessment

Organizations use a fraud risk profile or matrix to document their fraud risk assessments, as shown in the illustration in Figure 11. This fraud risk assessment matrix example provides an overview of a risk assessment's sequencing when looking at the column headings from left to right. The first column includes the identified fraud risks and schemes, which are then assessed for their relative likelihood and significance of occurrence (columns 2–3). Next, the risks and schemes are mapped to the personnel or departments involved and to existing fraud control activities (columns 4–5). Column 6 includes assessment of existing controls for design effectiveness and testing of existing controls to validate operating effectiveness. Finally, the organization identifies residual risks and develops a fraud risk response (columns 7–8) to address these residual risks.

Figure 11. Fraud Risk Management Assessment Matrix Example

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Financial Reporting • • •							
Non-Financial Reporting • • •							
Asset Misappropriation • • •							
Illegal Acts and Corruption • • •							

Column 8 provides the important linkage to the next step in the Fraud Risk Management Program — designing preventive and detective control activities that mitigate residual fraud risks. In subsequent risk assessments, the control activities included in column 8 of prior risk assessments are moved to column 5 and assessed for effectiveness. Through this iterative process, fraud risk management undergoes continuing improvement and strengthening. Appendix E shows this matrix completed for several possible fraud risks and illustrates how to use the matrix to document the fraud risk assessment.

Performs Reassessments and Assesses Changes to Fraud Risk

The risk assessment process is iterative rather than a one-time exercise. The risk assessment is conducted initially and then re-performed periodically. Every organization experiences change, and every change experienced has an impact on fraud risks.

The initial fraud risk assessment can be viewed as the "baseline" assessment. The periodic reassessments can be viewed as "maintenance" assessments.

Changes can occur due to factors over which the organization has no control (external changes); factors the organization can control, such as mergers and acquisitions or changes in operations (operational changes); and adjustments in key personnel (leadership changes).

The organization is alert for these types of changes and recognizes that any change results in the need for a new or updated fraud risk assessment related to areas that are affected by the changes.

It is important for everyone in the organization to be cognizant of the continuing nature of this process and the need to be aware of changes in the fraud risk environment, including new tools and techniques for fraud prevention and detection. Fraud risk management is best served if the focus comes from both the top down and the bottom up. In most organizations, this will require a cultural transformation in how the organization thinks about both fraud risk and the impact of fraud on the organization's reputation and ability to meet its objectives and goals. For employees, who may be inclined to think that this is top management's responsibility, fraud risks represent risks to their jobs if the organization suffers major reputational or financial losses.

External Environment Changes

Changes in the regulatory or economic environment can result in changes in the items about which regulators are most concerned and in the financial incentives and pressures facing an organization. The fraud risk assessment team maintains awareness of these changes and how the changes can affect their fraud risk assessment.

For example, changes in regulations affecting financial institutions may create new compliance requirements or forbid certain transactions. Employees may be incentivized or perceive pressure to hide transactions or falsify reports to appear as if they are adhering to new regulations. Changes in the economic environment could signal the beginning of an economic recession, and employees may perceive pressure to continue to meet earnings targets by reducing necessary reserves or allowances or by paying bribes to secure business.

The example below illustrates how an emerging external, non-financial reporting risk poses a significant fraud risk warranting careful focus and attention.

Example of Consideration of New and Emerging Fraud Risks: Environmental, Social, and Governance Initiatives and Reporting

Fraud and unethical behavior in Environmental, Social, and Governance (ESG) initiatives is a growing threat. For example, Volkswagen's diesel engine scandal remains one of the most notable incidents of fraud in business history. In another example, a massive Ponzi scheme was based on the fraudulent claim that biochar (waste from tires and household garbage) would be a future source of green energy. And a vast carbon credit fraud perpetrated on people in the UK led to the arrest and extradition of perpetrators. These high-profile incidents reveal a simple truth: When stakes are high, people are often willing to lie. ESG is no exception.

Regulators are already addressing the fraud potential in ESG initiatives. For example, the U.S. Securities and Exchange Commission (SEC) created a Climate and ESG Task Force to analyze data to identify potential violations and misconduct. It also created a web site to receive ESG-related tips, referrals, and whistleblower complaints.

When developing an ESG framework and culture, the process can be enhanced by asking these questions:

- Are my company's ESG disclosures subject to the same rigor as our financial disclosures?
- What are our management assertions about ESG, and are controls in place to ensure that these assertions are accurate and supported?
- What is our plan to disclose and correct ESG reporting problems?

Treating ESG with the same attention and importance as financial reporting can lead to more consistent focus on accuracy and integrity. The principles of fraud risk management are applicable to ESG reporting as well as to financial reporting in accomplishing these goals:

- Recognize the fraud risks associated with ESG initiatives and reporting.
- Assess the effectiveness of existing control activities.
- Devise and apply additional control activities to mitigate residual risk.
- Monitor continued adherence and compliance.

It is important to note that like accounting standards, ESG goals evolve, and companies will adapt and apply new methods of valuation and performance that require ongoing assessment and monitoring.

Operational Changes

Organizations regularly introduce new product lines or services or change the manner in which they process and report data. These changes can lead to new incentives and pressures on employees and new activities that need to be assessed for fraud risks.

For example, an organization may introduce a new product line, one about which management has predicted very promising financial results. If the new product sales are not meeting internal forecasts and budgets, employees may feel pressure or be incentivized to make it appear that the product launch is achieving success by reclassifying other product revenue as being attributable to the new product. They may also resort to making false claims about the product or paying bribes to retailer representatives to feature the product in their stores.

Similarly, organizations also may systematically outsource non-core activities. The fraud risk assessment team considers the impact of outsourcing initiatives on current employee morale as well as the activities being transferred to the outsource provider. The organization considers whether the outsource provider has adequate controls to address the fraud risks inherent in the services they are providing (e.g., a third-party processor of healthcare payments with access to sensitive data has controls in place to mitigate the related risks).

With accelerating advances in technology leading to new and innovative businesses and ways of doing business, organizations focused on fraud risk management will remain alert for inherent risks associated with these changes. For example, there could be inherent risk in interacting with organizations that are newly legal, and are subject to evolving legal and regulatory constraints.

Leadership Changes

Changes in leadership can bring changes in the tone at the top, which could affect the culture of compliance within an organization. Changes in leadership personnel throughout the organization can change the people who execute and approve transactions and provide oversight of the Fraud Risk Management Program. These new leaders may not fully understand the processes, controls, and monitoring activities in place at the organization. Consequently, employees, vendors, or customers may attempt to take advantage of this perceived lack of understanding and consider the change an opportunity to attempt to commit a fraud.

Changes in the Fraud Landscape

Organizations face evolving fraud schemes and risks, including the following risks:

- Cyber fraud, including techniques like phishing, and malware
- Identity theft-based fraud using stolen information and techniques like deepfake voice and video spoofing, image manipulation, and sophisticated counterfeit identity documents
- Ransomware and corporate extortion
- Blockchain and crypto-currencies, which open up new avenues for fraud, such as a 51 percent attack, and facilitate anonymous fraudulent activity
- Economic disruptions, business cycles, and the impact of natural events that attract fraud perpetrators exploiting them. Government programs designed to ameliorate these events may compound these risks. For example, with expanded unemployment benefits implemented as part of COVID-19 pandemic relief efforts came massive amounts of unemployment fraud across the United States
- Disruptive technologies and changes in business practices that may introduce new risks or open gaps in internal controls. For example, shifts to remote and hybrid work environments during the COVID-19 pandemic had fraud risk impacts that were hard to predict, categorize, and monitor
- Increased use of innovative tools by management that are executing accounting functionality (e.g., the use of data automation software and robotics process automations) is thereby changing the landscape of the accounting function and ultimately the fraud risk profile
- Virtual accounting procedures (such as observing inventory using remote-observation tools) and assuring the authenticity of accounting records and audit evidence in remote and virtual work environments

Consequently, an effective fraud risk assessment approach includes timely monitoring to identify the relevant changing fraud landscape. A practice of constantly monitoring media and other sources for new and evolving frauds and then asking the questions, "could this happen to or in our organization?" and "if so, do we have effective controls in place to prevent or early detect it?" will trigger updated risk assessments.

Once the organization has conducted an initial fraud risk assessment, the next phase of the Fraud Risk Management Program is establishing fraud control activities to either prevent frauds from occurring or detect frauds that occur as quickly as possible. Chapter 3 explains how organizations establish and implement preventive and detective control activities.

CHAPTER 3. FRAUD CONTROL ACTIVITIES

Chapter Summary

Chapter 2 explains how an organization performs a comprehensive fraud risk assessment. The culmination of that assessment effort is the identification of residual fraud risk and the resultant need for additional fraud control activities.

This chapter explains the next important phase of fraud risk management: designing and implementing fraud control activities designed to help prevent frauds from occurring or result in the early detection of frauds that are not prevented.

A fraud control activity is an action established through policies and procedures, often with data analytics components, 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 to either prevent fraud from occurring or to detect fraud quickly in the event that it occurs.

While fraud control activities can serve multiple purposes, they 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.

Fraud control activities are performed at varying levels in the organization and, in some cases, are a combination of both preventive and detective considerations. The range of fraud control activities varies by organization.

Fraud Control Activities Principle

This chapter addresses Principle 3 of a Fraud Risk Management Program. Principle 3 states:

Chapter introduces **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.

Relationship to the COSO 2013 Internal Control Framework

In addition to the requirement to assess fraud risk in COSO Internal Control Framework Principle 8 (*The organization considers the potential for fraud in assessing risks to the achievement of objectives*), each component of the COSO 2013 IC Framework is relevant to the consideration of the risk of fraud. Therefore, the principles discussed in this chapter about fraud control activities mirror those of the COSO 2013 IC Framework's control activities principles.

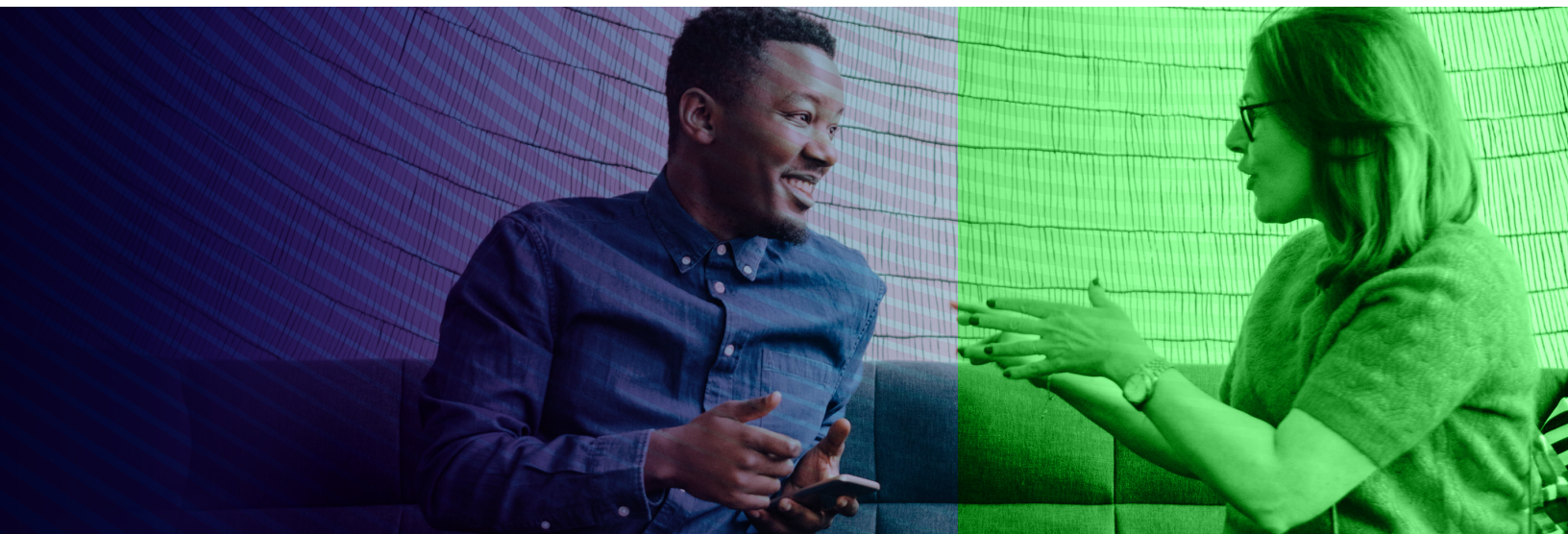
The COSO 2013 IC Framework, when read in conjunction with this chapter on fraud control activities, provides informative context regarding the topic of this chapter.

Fraud risk management Principle 3 correlates with the COSO 2013 IC Framework's components and principles as follows:

Figure 12. Fraud Risk Management Principle 3 Correlates with the COSO 2013 IC Framework's Components and Principles

COSO Framework Components and Principles		Fraud Risk Management Principle
Control Activities	**10.** The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**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.
	11. The organization selects and develops general control activities over technology to support the achievement of objectives.	
	12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	

While the COSO 2013 IC Framework's control activities principles are broadly designed to help ensure that management's directives to mitigate all types of risks to the achievement of objectives are carried out, fraud risk management Principle 3 focuses specifically on mitigating fraud risk.



Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- **Promotes Fraud Deterrence through Preventive and Detective Control Activities** — The organization addresses its fraud deterrence as a process of eliminating factors that may permit fraud to occur and understands that deterrence results from having effective preventive and detective fraud control activities in place.
- **Integrates with the Fraud Risk Assessment** — The organization ensures that the design and implementation of fraud control activities link directly to the fraud risk assessment.
- **Considers Organization-Specific Factors and Relevant Business Processes** — The organization ensures that the design and implementation of fraud control activities consider a range of factors, including factors unique to the organization, its industry, and its operating environment.
- **Considers the Application of Control Activities to Different Levels of the Organization** — The organization ensures that fraud control activities exist throughout the organization at all appropriate organizational levels.
- **Utilizes a Combination of Fraud Control Activities** — The organization ensures that fraud control activities include a range, variety, and mix of preventive and detective controls.
- **Considers Management Override of Controls** — The organization includes fraud control activities that consider and address the ability of senior management personnel to circumvent or override internal control activities, including fraud control activities.
- **Uses Proactive Data Analytics Procedures** — The organization implements a well-designed, rigorous system of data analytic processes and procedures that can identify **anomalous transactions** or events for further investigation. For many mid-to-large-size organizations, this may include the use of advanced data analytics techniques such as data visualization, text mining, machine learning, and statistical analysis.
- **Deploys Control Activities through Policies and Procedures** — The organization ensures that fraud control activities are thoroughly documented and implemented through organizational policies.

Promotes Fraud Deterrence through Preventive and Detective Control Activities

Deterrence is a broad concept that involves addressing the root causes that underlie the factors that contribute to fraud. Fraud deterrence is a process of mitigating factors that may cause fraud to occur. It is achieved when an organization:

- Establishes a visible and rigorous fraud governance process
- Creates a transparent and sound anti-fraud culture
- Reduces the opportunity for fraud by designing, implementing, and maintaining fraud control activities that are directly linked to the risks identified as a result of robust and thorough fraud risk assessments
- Takes swift action in response to allegations of fraud, including, where appropriate, actions against those involved in wrongdoing

One of the most effective fraud deterrents is an organizational culture that clearly communicates to its members through its words and actions that anyone attempting to commit fraud faces a high likelihood of getting caught and being held responsible and punished.

A **fraud preventive control** is a control activity designed to avoid a fraudulent event or transaction at the time of initial occurrence. Such control activities are specific processes and procedures designed to help eliminate the causes of fraud from occurring. Although it might be theoretically possible to design and implement fraud controls that would prevent all frauds, such controls would likely be too costly to be practical or too intrusive to business operations. Hence, **fraud detective controls** are also needed, as discussed below. For example, when there is a natural disaster or global pandemic, it may not be practically or physically possible to enforce a full range of preventive controls, given the need for rapid emergency response. This is not to say that a wide range of preventive controls should not be considered or deployed; but they must be balanced with the need to meet operational objectives.

A fraud preventive control is usually visible and generally known to employees or those with whom the organization interacts. Examples of such overt control activities include establishing procurement procedures and supervisory and managerial approval requirements. Preventive controls can be more successful if they are not widely known, or are covert control activities. A covert control activity is a control activity that is not readily apparent to employees or those with whom the organization interacts, e.g., data analytics designed to identify anomalous — and potentially fraudulent — transactions and prevent them from being processed.

A fraud detective control is a control activity designed to discover a fraudulent event or transaction after the initial processing has occurred. Such control activities are specific processes and procedures designed to identify attempted or existing frauds in a timely manner, thereby limiting the effects of any fraud that circumvents the organization's preventive controls. Although some detective controls are visible to selected employees who are responsible for them, these controls are usually most successful if they are covert.

Integrates with the Fraud Risk Assessment

Fraud control activities are an integral part of the fraud risk assessment component of an internal control system. A key element of the fraud risk assessment process (Chapter 2) is the identification of existing fraud control activities associated with and designed to address each specific fraud risk or potential fraud scheme. Consequently, at the conclusion of the fraud risk assessment process, each identified fraud risk is linked to an associated fraud control activity.

In some cases, following the initial fraud risk assessment, the risk assessment team may conclude that there are no existing controls for an identified fraud risk or potential fraud scheme. If the organization wants to reduce its fraud risk for that identified fraud vulnerability or potential fraud scheme, then management selects, develops, and implements control activities to mitigate those fraud risks.

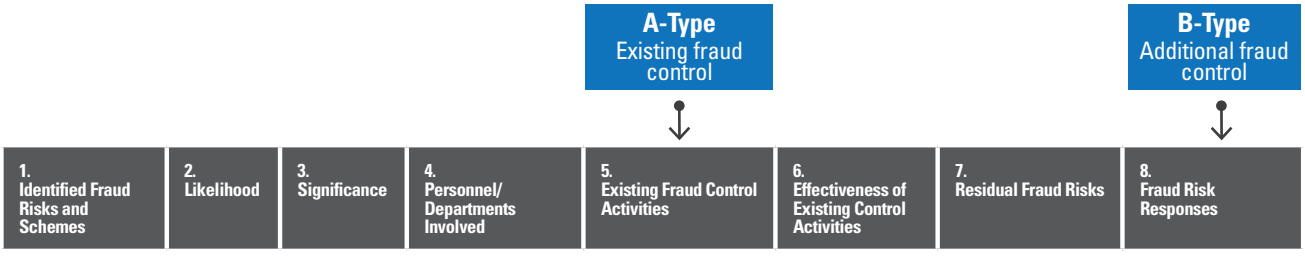
In some cases, the risk assessment team may conclude that there are some existing fraud control activities that are not sufficient to reduce fraud risk to an acceptable level. In those cases, management selects, develops, and implements *additional* fraud control activities to supplement or replace existing control activities.

The following illustration depicts the fraud risk assessment summary matrix and shows the two areas of the fraud risk assessment matrix in which control activities are identified:

- **A-Type** — Existing fraud control activities that are identified and linked to identified fraud risks and schemes
- **B-Type** — Additional fraud control activities developed as a response to unacceptable residual fraud risk

Residual fraud risk is the remaining risk that a fraudulent event or transaction will occur or not be detected in a timely manner after consideration of the effectiveness of existing control activities.

Figure 13. Fraud Risk Assessment Summary Matrix, Control Activities Areas



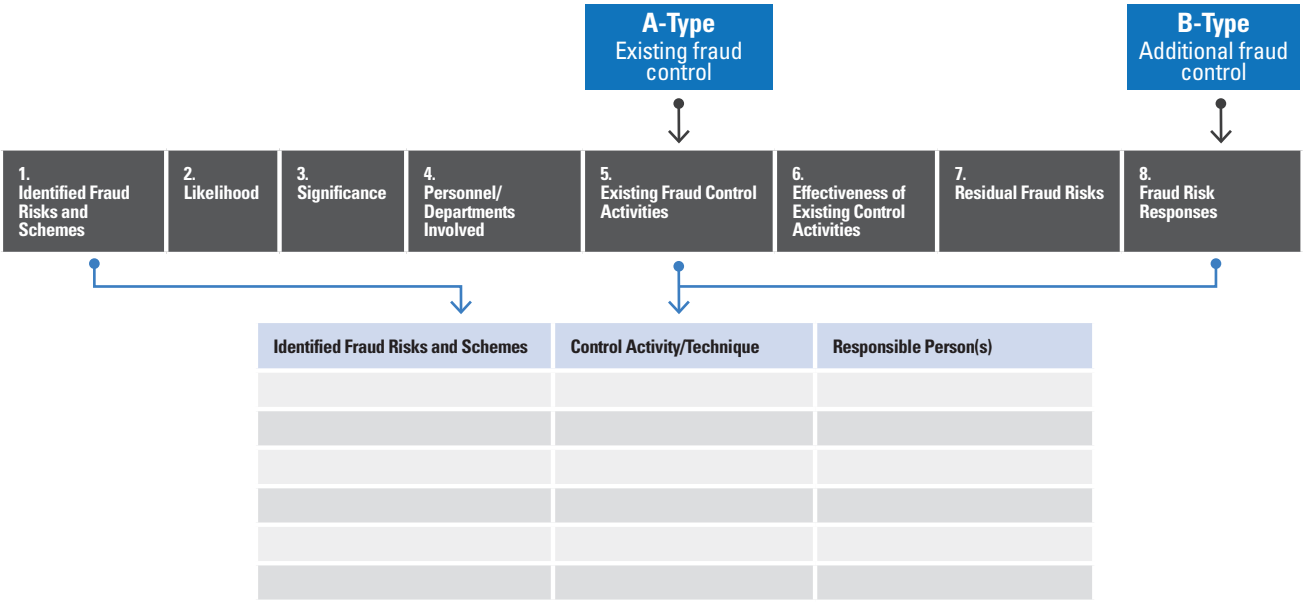
For example, the initial risk assessment might identify "employee might set up a phony vendor and process fraudulent transactions" as a potential fraud exposure. The assessment team might note that an existing control activity is that vendor accounts can only be established if a purchasing manager signs off on the data input form used to enter vendor information into the vendor data-base. Then, the assessment team might conclude that the existing control would not prevent someone from forging the manager's signature or prevent the purchasing manager from setting up a phony vendor. Finally, the assessment team would conclude that residual risk exists. An appropriate fraud risk response might include adding a new detective control activity, "on a monthly basis, use data analytics to look for matching information in the employee and vendor data-bases and identify who has created suspicious vendors."

As explained in Chapter 2, the fraud risk assessment process is performed initially and repeated periodically to address organizational growth and change as well as operating environment changes. In subsequent fraud risk assessments, the *additional* fraud control activities that had been identified in prior risk assessments would become *existing* fraud control activities. This ongoing fraud risk assessment process maintains the organization's Fraud Risk Management Program and allows it to become stronger and more effective over time.

Using the fraud risk assessment matrix, management develops fraud control activities and links them to the specific risks identified as part of the fraud risk assessment. Creating formal documentation of the link further enhances the completeness and accuracy of the assessment process.

As shown in the graphic below, in documenting fraud control activities, the initial column lists fraud risks and schemes taken directly from the risk assessment matrix and then lists, in the second column, fraud controls related to each risk. Some are existing (A-type) controls, and some are additional (B-type) controls. The third column identifies the person or persons responsible for ensuring that the control activity is being performed and remains effective.

Figure 14. Documenting Fraud Risk Assessment Summary Matrix, Control Activities Areas



Considers Organization-Specific Factors and Relevant Business Processes

The fraud risk assessment process considers and evaluates the potential fraud risks associated with business processes established across an organization to allow it to achieve its specific business objectives. As these business processes are largely developed and implemented by senior management of an organization, fraud risks can vary from organization to organization, even if organizations are in the same industry. Similarly, the selection and development of fraud control activities occur in response to organization-specific factors and relevant business processes.

This consideration also includes the organization-specific factors that could undermine the fraud control activities, including:

- Inconsistencies and weakness caused by people in the process
- Differences in judgment from person-to-person
- Time pressures
- Workarounds and overrides of controls
- Incentives and rewards that might run counter to control objectives

Organizations differ. Responses to fraud risk consider these differences.

Considers the Application of Control Activities to Different Levels of the Organization

Control activities are applied at various points, both organizationally and operationally. Preventive controls are usually more effective if applied early in business processes and at the lowest applicable organizational levels. Detective controls can be effective at various organizational and operational levels. The timing for a preventive control occurs before the initial occurrence. For example, a fraudulent transaction is not approved or completed because of a preventive control activity. In the case of a disbursement, organizations want to avoid a pay-and-chase situation. In contrast, a detective control identifies a fraudulent event or transaction after occurrence. A key element is that the detective control identifies the fraudulent event or transaction in a timely manner. Therefore, there can be varying times throughout the business process at which controls can be established to detect such events.

The ACFE's biennial study *Occupational Fraud: A Report to the Nations on Occupational Fraud and Abuse* consistently shows that managerial fraud that can lead to fraudulent financial reporting tends to result in significantly greater damage to an organization than misappropriation of assets or other non-financial fraud by lower-level employees. Thus, it is beneficial for organizations to pay special attention to control activities surrounding senior management actions and transactions initiated by senior managers.

In governmental organizations, program fraud, such as benefit recipient, healthcare provider, procurement, and tax fraud, may create the greater damage and be more visible to the public, thereby eroding trust in government.

Utilizes a Combination of Fraud Control Activities

Fraud and misconduct can occur at various levels in any organization as well as external to the organization. Therefore, it is essential that the mix of preventive and detective controls is sufficient to address the points in the process at which a fraudulent event could occur and those separate points at which a detective control could identify its occurrence in a timely manner. In many cases, a fraud control activity can include a combination of both preventive and detective considerations.

The design and implementation of these fraud control activities is a coordinated effort by management, generally supported by personnel representing all significant business processes across the organization.

Collectively, this cross-section of the organization generally is able to address all of the identified risks, design and implement the control activities, and ensure that the techniques used are adequate to mitigate the risk of fraud in accordance with the organization's fraud risk tolerance. Again, fraud risk tolerance is the level of residual fraud risk that an organization is willing to accept that a fraudulent event or transaction will occur and not be detected in a timely manner. Fraud risk tolerance recognizes that it is not possible to eliminate all fraud risk in organizations.

If the fraud risk assessment process reveals unacceptable residual fraud risk, management can evaluate and select appropriate fraud control activities. Multiple control activities, even those that are redundant or overlapping, can be helpful in managing risks with a high likelihood or a significant potential impact, in addition to those that are evolving rapidly (e.g., cybersecurity risks.) However, controls come with a cost, i.e., the direct cost of the control procedures themselves as well as the potential costs to the organization in terms of their effect on and possible interference with operations. Hence, when evaluating potential control activities to apply to mitigate residual fraud risk, the organization considers such costs to arrive at the optimum mix of preventive and detective controls.

Utilizing Fraud Preventive Control Activities

Prevention is the most proactive fraud-fighting measure. The ongoing success of any fraud prevention program depends on its periodic communication and reinforcement. Stressing the existence of a fraud prevention program through a wide variety of media, such as emails, webcasts, posters on bulletin boards, flyers, or electronic messages included with invoices and vendor payments, and articles in internal and external communications, gets the message out to both internal and external communities that the organization is committed to preventing and deterring fraud.

Fraud preventive controls generally fall into the following broad areas:

- Business process control activities, such as determining how to structure and manage operations; identifying ways to delegate authority and responsibility; considering whether to centralize or decentralize processes; considering whether to engage in outsourcing or to keep production in-house; and determining whether to subcontract.
- Physical access controls related to access to facilities, assets, and information systems.

- Logical access controls related to an organization's utilization of technology and information systems environment(s), e.g., employing the "right of access" to ensure that only those that have a "need to know" have the "rights to know."

- **Transaction-level control procedures** directly support the actions to mitigate transaction-processing risks in an organization's business processes. Transaction controls can be manual or automated and likely cover the information-processing objectives of completeness, accuracy, and validity. Such control activities include performing edit, completeness, and reasonableness checks; establishing procurement procedures; emphasizing documentation requirements; and establishing supervisory and managerial approval requirements.

- Technological control activities that support the other fraud preventive control activities provided in this listing might include third-party due diligence checks against known credit, sanctions, criminal or watch list data-bases, use of software-based fraud risk awareness training, and automated business rules or risk-scoring mechanisms that restrict certain business activities from occurring, such as escalating or stopping payments that are deemed high risk or out of policy before they are paid.

In any of these areas, controls can be designed and implemented at different levels of the organization. For example, the organization decides the required thresholds for higher-level approval requirements for specific transactions. Requiring more senior personnel to approve transactions above specified dollar thresholds can prevent unauthorized purchases from favored or related-party vendors. However, such controls also can lead motivated individuals to engage in purchase-splitting, i.e., dividing an above-the-threshold-limit purchase into smaller amounts to avoid the higher-level approval controls. Recognizing this, the organization can implement data analytic controls, such as stratifying the contract amount to identify patterns of payment activities just below a certain dollar threshold.

Among the most important elements supporting fraud prevention are human resources (HR) procedures, authority limits, transaction-level control procedures, and oversight designed to prevent management override of controls. These elements can cut across all five of the preventive control activities explained above.

Utilizing Fraud Detective Control Activities

Having fraud control activities in place and visible is one of the most effective deterrents to fraudulent behavior. Of course, some controls are more effective as covert, rather than overt, controls. Deterrence can still be achieved if it is known within the organization that covert controls are being carried out. As with preventive controls, it is important that the organization assess and continuously monitor its detective controls to determine that fraud detection techniques are present and functioning. (See Chapter 5 for a discussion of Principle 5 related to monitoring the Fraud Risk Management Program.) This assessment helps ensure that transactions with a higher risk of fraud are detected in a timely manner. Also, through detective controls, management gains a better understanding of the organization's fraud risks, which will assist in strengthening preventive controls.

The types of specific detective controls implemented depend on the fraud risks identified. For example, if an organization operates in countries identified as having high risks for corruption, it may implement detective controls to identify possible violations of the Foreign Corrupt Practices Act (FCPA), such as a recurring review of expense reports or consulting fees. Similarly, if an organization's financial statements rely on a high frequency of subjective estimates, it may implement monthly review of the estimates by an objective, competent reviewer. Otherwise, certain people who are motivated to commit fraud might see an opportunity to override or evade a control or collude with others to do so. Therefore, detection techniques are flexible, adaptable, and continuously evolving to meet changes in risk.

While preventive controls are often apparent and readily identifiable by employees, third parties, and others, specific detective controls are often covert in nature. The general knowledge within the organization that detective controls are present and functioning can serve as a strong fraud deterrent. Access to knowledge regarding the exact nature and specific design of detective controls is carefully controlled. Detective controls operate in a background that is not evident in the everyday business environment and often:

- Occur in the ordinary course of business

- Draw on external information to corroborate internally generated information

- Routinely and automatically communicate identified deficiencies and exceptions to appropriate leadership

- Use results to enhance and modify other controls

Although every organization is susceptible to fraud, it is not cost-effective to try to prevent all fraud. An organization may (if approved by the governing board) choose to design some of its controls to detect, rather than prevent, certain frauds. If the estimated costs of designing, implementing, and monitoring preventive controls against fraud (such as tools, personnel, or training) exceed the assessed impact of the risk, some specific preventive controls may not be cost-effective to

implement. A conscious decision to by-pass costly preventive controls needs to be coupled with detective controls that will early detect and remediate fraudulent transactions before a fraud grows to a harmful level.

An organization might decide to put carefully designed detective controls such as data analytic procedures in place to trigger a follow-up investigation of anomalous trends rather than impose costly or intrusive controls designed to prevent every fraudulent transaction. In conducting the fraud risk assessment, the assessment team considers both the probability of occurrence (likelihood) and impact (significance) of fraud risk exposures, and evaluates the availability of data for use in ongoing monitoring. In such cases, important detection methods also might include an anonymous reporting mechanism, such as a whistleblower system, process controls, and other proactive fraud detection procedures specifically designed to identify fraudulent activity if it occurs.

Utilizing Human Resources Procedures

An organization's HR function can play an important role in fraud prevention by implementing the following procedures.

Perform Background Investigations

A key business and fraud risk in any organization lies with the people who are hired to operate the business and with those who are promoted into positions of trust and authority. For that reason, it is important to know employees well enough to enable supervisors to evaluate their credentials and competence, match skills to the job requirements, and be aware of any issues of personal integrity that may affect their suitability for the position.

Much can be learned about an individual through confirmation of work history and education presented on a job application or résumé and in follow-up communications with references provided. Such procedures might uncover false or embellished information or undisclosed history and reputation that may represent increased, and possibly unacceptable, risk.

While the organization establishes procedures to obtain sufficient information to assess a job applicant or promotion candidate, the nature and extent of information that can be requested from a prospective or existing employee or obtained independently is governed by applicable laws and regulations. Further or enhanced background checking for criminal record or personal financial situation may be possible only upon receiving the individual's consent. There is benefit in seeking legal counsel regarding what background information can and cannot be obtained and the appropriate procedures to follow.

In addition to background checks as part of the initial hiring process, the organization may want to consider periodic updated background checks of key individuals to be able to identify and evaluate changed circumstances that indicate heightened fraud risk. Similarly, considering updated background checks whenever behavior red flags are noted with respect to existing employees or management personnel is important.

Considering updated background checks whenever behavior red flags are noted

According to the ACFE biennial *Report to the Nations on Occupational Fraud and Abuse*, around 90% of fraud perpetrators also exhibited at least one behavioral red flag (living beyond means, financial difficulties, unusually close relationship with a vendor or customer, control issues, and so forth).

Background checks for new and existing suppliers, customers, and business partners also can help identify any issues of financial health, ownership, reputation, and integrity that may represent an unacceptable risk to the business.

Provide Fraud Risk Management Training

An organization hires or promotes competent individuals who, having undergone appropriate background checks, represent a low initial fraud risk. If all employees at all levels receive an initial orientation and ongoing education on the Fraud Risk Management Program, these actions establish and reinforce the tone from the top regarding each individual's responsibility to help prevent and detect fraud, as well as the process to deal with suspected or observed fraud. ACFE's research has consistently shown that organizations with anti-fraud training have lower dollar losses due to fraud and frauds that do happen are discovered more quickly.

An organization's HR group is sometimes responsible for developing and providing the necessary training on the purpose of the Fraud Risk Management Program, including the codes of conduct and ethics, what constitutes fraud, and what to do when fraud is suspected or observed. In some cases, this responsibility is given to the organization's legal group or ethics officer. Ideally, however, staff members who are integrally involved in the Fraud Risk Management Program — preferably stakeholders who are deemed responsible for the success of the program — work with that implementation group to ensure this training reflects the specific fraud risks, operations, and circumstances of the organization. Mandatory attendance for fraud-related training sessions, including periodic updates and refresher sessions is important. A signed affirmation from every

employee on an annual basis that he or she is aware of the organization's code of conduct, will continue to comply with the code of conduct, and is aware of the organization's Fraud Risk Management Program ensures that employees remain aware of the organization's important fraud preventive control mechanisms.

Evaluate Performance and Compensation Programs

Human resource managers also are generally involved in both performance management and compensation programs. Performance management involves the evaluation of employee behavior and performance as well as work-related competence. It is a human trait to want recognition and rewards for competence and positive performance. Regular and robust assessments of employee performance, with timely and constructive feedback, reinforce positive attributes and prevent potential problems.

Employees who are not recognized for what they do and what they have accomplished, especially those who may have been bypassed for promotions or compensation increases, may be more likely to rationalize that fraudulent conduct is justified.

Reward also can be reflected in compensation. By conducting compensation surveys and local market analysis, HR can determine whether senior management and employees are compensated within a competitive range. Additionally, the structure of the compensation system (e.g., the balance between fixed and variable compensation) is evaluated to determine whether desired behavior is being incentivized properly. For example, managers whose compensation is largely based on short-term, performance-related bonuses may be motivated to cut corners or deliberately fabricate financial results to achieve those bonuses.

Measure and Monitor Corporate Culture

Organizations may measure and monitor a variety of indicators of corporate culture, including employee attrition and absence rates, performance and feedback processes and data, dismissals and reprimands, information from employee focus groups, employee surveys, exit interviews, and others.

Organizations often conduct annual surveys of their employees to obtain feedback on certain qualities associated with the organization as a whole and with the employee's specific area of responsibility and management team. These surveys are often administered by the organization's HR department and seek feedback in areas such as the organization's strategy, customer experience, products and services, leadership, work environment, work-life integration, opportunity and development, and transparency and distribution of information.
Feedback related to integrity within the organization is especially valuable. Attributes that can be assessed in this section of the survey can include:

- Employee knowledge of the organization's Fraud Risk Management Program
- Employee ability to report unethical behavior or practices without the fear of retaliation
- The effectiveness of the organization's responses to verified or proven unethical behavior
- Any observed misconduct in the past year and whether such misconduct was reported
- Employee knowledge of how to report ethical concerns or observed misconduct

The organization evaluates all identified areas of weakness and specific concerns raised within the organization to allow it to remediate such issues.

Conduct Exit Interviews

A policy of conducting written or oral exit interviews of terminated employees or those who have resigned can help in both fraud prevention and detection efforts. These interviews help the organization identify issues regarding management's integrity or information regarding conditions that might be conducive to fraud. Appropriate members of management review the content and information contained in exit interviews and resignation letters, because they may contain information regarding possible fraud and misconduct existing within the organization.

Exit interview questionnaires and conversations can assist management in obtaining information about fraud. For example, in seeking fraud-related information from an exiting employee, the exit interview could include the following question: "Did you ever observe what you considered to be dishonest, unethical, or fraudulent behavior?" If departing employees answer such a question, potential dishonest, unethical, or fraudulent activities could be identified for follow-up and remediation.

Implement Segregation of Duties

Careful segregation of duties to ensure that single individuals do not have responsibility or authority for all steps in a business process is one of the strongest fraud risk management controls. When selecting control activities, an organization uses segregated duties to as great an extent as possible. A general rule is "three deep," meaning, for example in the purchasing function, the person that requests the item, does not authorize its purchase, verify receipt, nor authorize its payment.

Organizational changes, including changes in organizational structure or operational processes, warrant analysis of segregation of duties, especially in smaller organizations or smaller operating units within larger enterprises.

Nevertheless, the intended effects of duty segregation control activities can be nullified by collusion. Consequently, organizations can reduce the risk of collusive fraud with regular rotation of duties among personnel and establishment of mandatory leave policies. The use of data analytic procedures can help identify anomalous transactions that might indicate collusion and identify employees who rarely take leave.

Establish Authority and Responsibility Limits

Fraud is less likely when an individual's level of authority is commensurate with his or her level of responsibility. A misalignment between authority and responsibility, particularly in the absence of control activities and segregation of duties, can lead to fraud.

For example, if an office or branch manager with the authority to directly hire new employees decides to hire friends at salary levels that are inconsistent with the friends' qualifications in return for kickbacks, that misalignment between authority and responsibility is problematic. The same outcome results if that manager places ghost employees on the organization's payroll. Appropriate oversight or segregation of duties (e.g., requiring someone other than the manager to approve salaries and to set up the new employee in the payroll system) can mitigate the risk of such occurrences.

Authority and responsibility authorizations can become outdated or otherwise inappropriate due to changes in employment status, promotions, reassignments, and terminations. Hence, these authorizations need to be re-evaluated periodically.

Implement Transaction-Level Control Procedures

Transaction-level control procedures generally pertain to how to process individual transactions.

They include data entry edit tests, segregation of transaction-processing duties, authorization approvals, etc. Higher level reviews and approvals may be appropriate for transactions that are potentially problematic, including **related-party transactions**, end-of-period adjustments, or management-initiated journal entries.

Because fraud schemes often involve the use of third-party entities or individuals, organizations need thorough authorization and approval controls so that such relationships cannot be exploited to perpetrate fraud.

Accounting adjustments occurring just before or just after important closing dates deserve special scrutiny to ensure that they are valid and appropriate. Journal entries, particularly those initiated by senior managers or officials, also warrant special attention. These entries could be indicative of management override of controls.

Preventive controls are important for any transactions that can be influenced by board members or senior executives or controlled by employees with authority who have an interest in an outside organization with which the organization may conduct business. Such individuals may influence or mandate transactions that ultimately benefit them at the expense of the organization.

Utilize Whistleblower Systems

A ***whistleblower*** is a person who alerts someone in a position of authority to an instance of wrongdoing, such as unethical conduct, a legal violation, or fraud. Establishment of a comprehensive whistleblower or hotline reporting process is one of the most important fraud detection controls an organization can have. Further, knowledge within the organization that such a reporting system exists can be one of the strongest deterrents against fraud. ACFE research consistently reveals that tips, often from employees or anonymous sources, are the single greatest source of detected frauds. In certain jurisdictions, whistleblower systems may not be legal or may be subject to restrictions. As such, multinational organizations may not be able to implement such systems on a worldwide basis. To ensure that whistleblower systems comply with all regulations and restrictions, consultation with legal counsel is important.

Why are communication and reinforcement important in a fraud prevention program?

According to the ACFE research presented in *Occupational Fraud: A Report to the Nations*, more fraud is detected by tip than by any other source, with more than half of the tips reported by employees. (ACFE.com/RTTN)

A comprehensive whistleblower reporting system is a vital part of a holistic Fraud Risk Management Program that serves as both a detective and preventive measure. Whistleblower reporting systems are discussed in greater detail in Chapter 4, Fraud Investigation and Corrective Action.

Considers Management Override of Controls

In all but a few cases, catastrophic frauds in the past were perpetrated by senior management officials. Reform efforts of the early part of this century increased the importance of governing boards' role. Oversight controls assist those charged with governance in holding senior management accountable, in preventing, and in promptly detecting instances in which management attempts to override or circumvent control procedures to commit fraud.[13]

Some controls focus on improper transactions that benefit managers, such as direct payments to senior managers and related parties. Other controls focus on senior managers' ability to manipulate financial reporting processes. For example, one of the methods that senior managers can employ to circumvent internal control over financial reporting is the use of journal entries. Accordingly, organizations have control activities in place to prevent improper transactions through top-side adjustments to accounting information by managers.

Other ways in which management may attempt to override controls is by applying inappropriate bias in their assumptions underlying accounting estimates, entering into unusual and fraudulent transactions near period-end to meet their objectives, or pressuring subordinates to initiate or participate in improper transactions or activities.

Robust fraud risk assessments address potential areas for management to intentionally manipulate the financial statement close process and other aspects of financial reporting.

Uses Proactive Data Analytics Procedures

Data analytics can identify anomalous transactions and risk indicators from among data sets, large and small. Users of data analysis may be able to examine journal entries looking for suspicious transactions, such as those occurring at the end of a period, those occurring outside normal operating hours, or those made in one period and reversed in the next period. Data analysis also may allow users to look for journal entries that fraudulently credit expense accounts to improve net income to meet analysts' expectations or employee incentive compensation targets.

Moreover, data analysis allows users to identify anomalous relationships among people, organizations, and events, leveraging data obtained both within the organization as well as externally obtained, e.g., social media feeds or sanctions or watch list data-bases.

In most organizations, data analytics are used in almost every business function — from sales to marketing, contracting, finance, engineering, human resources, and management. However, data analytics also play a key role in prevention and detection of potentially improper procurement transactions, payments, sales, or rogue employee behavior.

Some of the common areas where proactive data analytics procedures are used to help prevent and detect misconduct or fraudulent activity are around vendors, employees, and customers. As such, aligning to those business processes is key to using data analytics for proactive monitoring. Specific examples of this approach include the following:

- **Accounts Payable, Procure-to-Pay function —** Proactive data analytics can prevent an improper or fraudulent payment, avoiding the difficulties of trying to recover from a rogue vendor after they have the money. Through risk scoring, visualization, and other advanced techniques discussed in Appendix D, procure-to-pay analytics can efficiently prevent and detect potential fraudulent activity. Top-level accounts payable statistics provide only a superficial analysis of payments. Analyses that review accounts payable subledger payment and invoice details are more likely to find potentially improper payments. Analysis of the vendor master files, due diligence checks on the vendor, and vendor questionnaires or contracts are also helpful data sources when modeling and designing procure-to-pay tests. There are many variations of asset misappropriation, corruption, and financial misstatement schemes that can involve improper payments.
- **Employee Travel & Entertainment (T&E) expenses —** T&E transactions can be high-risk because they often rely on personal judgment as to whether an expenditure is acceptable and reimbursable. However, the sums involved can be relatively low compared to other business transactions. In many cases, the amount and vendor are not the only important attributes. Business context can also be important, such as whether the transaction related to a political or government official, involved a family member or friend, or had an unclear business purpose. Even small transactions can be important if they involve a senior executive. Bribe payments, for example, may result in prosecution even when they are financially immaterial.

[13] See *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention.*

- **Accounts Receivable, Order-to-Cash function —** The Order-to-Cash function — including sales, discounts, timing of shipments, returns, credits, and rebate transactions — is susceptible to asset misappropriation, corruption, and revenue recognition and other financial reporting fraud schemes. Customer-level monitoring often focuses on knowing the customers and identifying excessive returns, free goods, or unusual discounts.

- **Regulatory compliance —** Proactive data analytics can help companies screen for transactions and business conduct that run afoul of industry-specific regulatory compliance requirements. For example, pharmaceutical companies may screen for sales-related entertainment of healthcare providers that might violate regulations or require public disclosures. In another example, financial institutions may screen depositors and transaction flows to identify interactions with depositors or transferees on watch lists of those suspected of trafficking or terrorist financing.

- **Data protection and privacy —** As part of a comprehensive Fraud Risk Management Program, coordination with information security professionals is an important element to not only secure the information assets of the organization, but also to ensure that the data analytics procedures used within the organization do not present any risks with respect to applicable data privacy regulations.

The details of what constitutes an effective information security environment are beyond the purpose of this document. For information about cyber risks and the security environment, see *COSO guidance on Managing Cyber Risk in a Digital Age*.

Cybersecurity and data protection breaches are not just information security or information technology concerns. They are fraud risk concerns, because weaknesses in them can allow fraud, including intentional acts designed to misstate financial information, misstate non-financial information, and misappropriate assets. And, of course, cyber fraud and cybersecurity breaches are illegal acts.

Continuous or real-time data analytics can speed identification and reporting of potential fraudulent activity. For example, a Benford's Law analysis can examine expense reports, general ledger accounts, and payroll accounts for unusual transactions, amounts, or patterns of activity that may require further analysis. Similarly, continuous monitoring of transactions subject to certain "flags" can enable investigation of higher-risk transactions as soon as they occur.

Technology tools enhance the ability of management at all levels to prevent, detect, and deter fraud. Tools, like data analysis, data mining, and digital analysis can be used to:

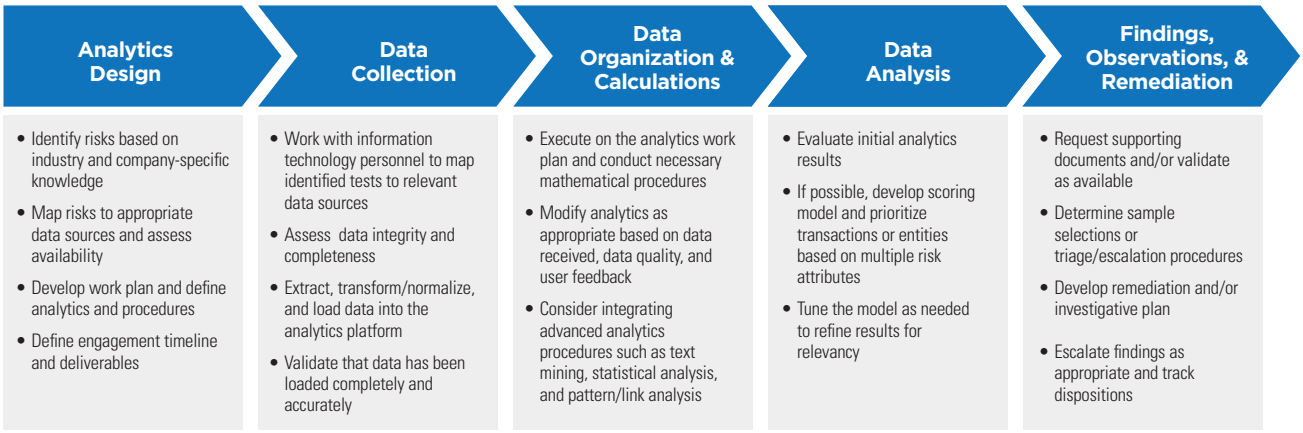
- Identify hidden relationships among people, organizations, and events
- Identify suspicious transactions
- Assess the effectiveness of internal controls
- Monitor fraud threats and vulnerabilities
- Consider and analyze thousands or millions of transactions

Proactive consideration of how certain fraud schemes may result in identifiable types of transactions or trends enhances an organization's ability to design and implement data analysis. ACFE research has consistently shown that the use of proactive data analytics also can ensure the cost-effectiveness of other fraud preventive and detective controls, often decreasing both the cost of the fraud to the organization and the duration of the scheme.

In general, it is helpful to take an iterative approach to the use of proactive anti-fraud data analytics procedures to ensure that the tests are designed and tested carefully and then continuously monitored and improved. Such proactive procedures do not always require the use of expensive software. Further, many proactive anti-fraud data analytics procedures described in this section can be utilized during an investigation in which specific fraud-related allegations are present. (See Chapter 4 for more information on investigations.)

While the scope of this document is not intended to be all-inclusive with respect to data analytics considerations, the graphic below sets forth a framework displaying how to arrange an analytics work plan in five distinct phases.

Figure 15. Example of a Data Analytics Framework



A more detailed discussion of each phase and the topics related to data analysis is available in Appendix D-2.

Deploys Control Activities Through Policies and Procedures

Formal documentation of an organization's fraud risk management policies and procedures, those control activities developed to prevent and detect fraud, is important. This documentation includes the processes used to monitor the performance of fraud control activities and indicates when such controls are not sufficient to reduce fraud risk to an acceptable level. Testing procedures conducted to determine that controls are present and functioning as designed ensure adequate operation of fraud control activities. These procedures and the test results also are important enough to be thoroughly documented.

Although the organization may want to describe and explain some aspects of its fraud detection techniques to its employees, vendors, and stakeholders, certain aspects of the plan remain confidential. For example, during the fraud detective control development phase, participants are warned to keep such information confidential. The board approves a specific list of individuals who are permitted access to the information and defines its own level of information access related to fraud detective controls.

Once the final fraud risk management plan is completed, the team develops communications regarding the plan and its implementation. Knowledge throughout the organization that a comprehensive fraud risk management plan exists is, in and of itself, a strong deterrent. By communicating this information to employees, customers, vendors, shareholders, and others, the organization affirms that it has a fraud risk management plan in place and that it takes fraud seriously, without revealing all the relevant characteristics of the organization's fraud detection techniques included in the plan.

Responsibility and Accountability

Documentation of the policies and procedures includes not only what will be done, but who will do it, including both a detailed description of the elements of the organization's fraud prevention and detection activities and techniques and the roles and responsibilities of all parties involved. Organizations designate and document the individuals and departments responsible for:

- Designing and planning the overall fraud prevention and detection processes
- Designing and implementing specific fraud preventive and detective controls
- Monitoring specific fraud preventive and detective controls and the overall system of these controls for realization of the process and program objectives
- Receiving and responding to all reports related to possible fraudulent activity in a timely manner
- Investigating all reports of fraudulent activity in a timely manner
- Communicating information about suspected and confirmed fraud to appropriate parties in a timely manner
- Periodically assessing and updating the plan for changes in technology, processes, and organization as well as lessons learned from the analysis

Implementation

As in any control activity, implementation procedures include the timing of the fraud control activity and any follow-up corrective actions. Similarly, when a fraud control activity identifies a matter for follow-up, investigating that matter and taking appropriate action is important. Finally, a well-designed fraud control activity plan includes a requirement for competent personnel with sufficient authority to perform the fraud control activity.

Reassessment

To strengthen policies and procedures, organizations beginning to implement a Fraud Risk Management Program, as well as those striving to improve their Fraud Risk Management Program, benefit from conducting overall assessments of their policies and procedures for fraud control activities. (See Appendix F for descriptions of and links to resources that include the Fraud Control Activities Scorecard that provides further information about this process and its terminology.)

Periodically reassessing their fraud control activities ensures organizations that progress is being made to arrive at an "all-green" fraud control activities status and that no elements of fraud prevention and detection are deteriorating. Periodic reassessments include:

- Ensuring that existing fraud control activities are working as designed
- Refreshing and updating the fraud risk assessment and the design of control activities
- Seeking efficiencies and filling gaps

Reassessments occur on both a scheduled basis and at every significant change in the organization, its operations, or in the environment in which the organization operates. Organizations with strong commitments to fraud risk management also may wish to engage independent outside experts to assess their fraud prevention and detection techniques.

Once the organization has conducted an initial fraud risk assessment and designed and implemented appropriate fraud control activities, the next phase of the Fraud Risk Management Program is establishing mechanisms to investigate potential frauds and take swift and appropriate corrective action when fraudulent activity is suspected or determined. Chapter 4 explains this next important aspect of fraud risk management.

CHAPTER 4. FRAUD INVESTIGATION AND CORRECTIVE ACTION

Chapter Summary

Chapter 3 addressed designing and implementing preventive and detective control activities. Such control activities, however, 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 noncompliance and allegations involving fraud and misconduct. This chapter explains how to collect information about potential fraud and how to carry out investigation and corrective action steps.

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.

The governing board and senior management establish a process to evaluate allegations of fraud and misconduct. Individuals assigned to investigations have the necessary authority and skills to evaluate the allegations and determine the appropriate course of action. The process includes a tracking or case management system that records and tracks all allegations until they are resolved. With respect to allegations involving senior management, the board becomes actively involved.

After an initial evaluation of an allegation, if an investigation is warranted as the next course of action, the board ensures that the organization has an appropriate and effective process to investigate allegations and maintain confidentiality. A comprehensive and consistent process for conducting investigations can help the organization mitigate losses and manage risk associated with the investigations.

Consulting legal counsel is advisable before undertaking an investigation to protect legal privileges as well as work product. In some states, investigations may be conducted only under the direction of counsel. Outside the United States, some jurisdictions require obtaining permission from government authorities before commencing an investigation. Counsel is involved in providing legal advice before taking or pursuing disciplinary and civil actions as well as making criminal referrals. As a matter of good governance, as described more thoroughly in the first chapter of this Guide, management and the board ensure that these measures are in place as important aspects of a **fraud response plan**.

In accordance with policies approved by the board, the investigation team reports its findings to the appropriate party, such as senior management, directors, legal counsel, and oversight bodies. Public disclosure to law enforcement, regulatory bodies, investors, shareholders, the media, or others may also be warranted or required in some cases.

If certain actions are required to preserve evidence, maintain confidence, or mitigate losses before the investigation is complete, those responsible ensure that there is a sufficient basis for those actions. When access to computerized information is required, those responsible take appropriate steps to ensure the continuing integrity of the information. In addition, they consider whether there is a need for specialists trained in electronic file preservation.

Actions taken are appropriate in the circumstances and are consistently applied to all levels of employees, including senior management and board members. Those responsible take such actions only after consultation with human resources (HR), legal counsel, and individuals responsible for such decisions.

Fraud Investigation and Corrective Action Principle

This chapter addresses principle 4 of a Fraud Risk Management Program. Principle 4 states:

Chapter introduces **Principle** 4

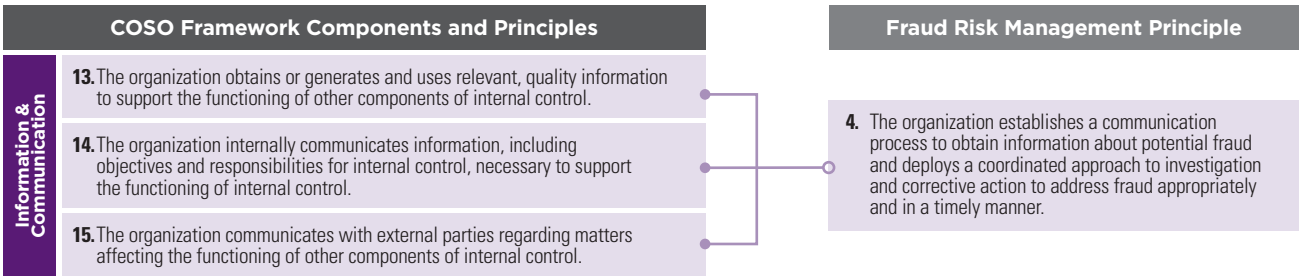
The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

Relationship to the COSO 2013 Internal Control Framework

In addition to the requirement to assess fraud risk in the COSO 2013 IC Framework Principle 8 (*The organization considers the potential for fraud in assessing risks to the achievement of objectives*), each component and principle of the COSO 2013 IC Framework is relevant to the consideration of the risk of fraud. Therefore, the principle discussed in this chapter about fraud investigation and corrective action mirrors the COSO 2013 IC Framework's information and communication principles. The COSO 2013 IC Framework, when read in conjunction with this chapter on fraud investigation and corrective action, provides informative context regarding the topic of this chapter.

Fraud risk management Principle 4 correlates with the COSO 2013 IC Framework's components and principles as follows:

Figure 16. Fraud Risk Management Principle 4 Correlates with the COSO 2013 IC Framework's Components and Principles



The COSO 2013 IC Framework's information and communication principles are broadly designed to help ensure that the organization has appropriate information and communication mechanisms in place with respect to all aspects of internal control. Fraud risk management Principle 4 is more narrowly focused on establishing the information and communication, investigation, data analysis, reporting, and corrective action processes related specifically to fraud.

While each of the three COSO information and communication principles is consistent with and supportive of Fraud Risk Management Principle 4, this principle focuses specifically on obtaining information about potential fraud and on investigative and corrective actions related to potential fraud.

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- **Establishes an Effective Whistleblower Reporting System** — The organization establishes, supports, and promotes a system designed to gather information from employees and other stakeholders about observed or suspected wrongdoing.
- **Establishes Fraud Investigation and Response Protocols** — The organization establishes, formally documents, and maintains a process for the receipt, evaluation, and treatment of communications of potential fraud.
- **Conducts Investigations** — The organization undertakes investigations of potential fraud, giving due consideration to the scope, severity, credibility, and implications of the communicated matter.
- **Performs Data Analytics** — The organization undertakes data analysis to identify the underlying control weaknesses and the quantifiable loss (impact) of the potential fraud.
- **Communicates Investigation Results** — The investigation team communicates the results of the investigation to the appropriate internal authority and, when necessary, to external third parties.
- **Takes Corrective Action** — The organization selects discipline, remediation, asset recovery, or other activities to address the findings of the investigation.
- **Evaluates Investigation Performance** — The organization performs evaluations periodically to provide objective feedback on the effectiveness of the investigation process.

Establishes an Effective Whistleblower Reporting System

A whistleblower is a person who alerts an organization to an instance of wrongdoing, such as unethical conduct, a legal violation, or fraud. An important gauge of the Fraud Risk Management Program's success is how free employees feel to raise questions and concerns about the company or its personnel's actions. Implementing a whistleblower system, including one or more reporting channels such as a hotline, web line or website, email address, chatbot, or mobile application ("mobile app") to receive reports in the local business languages utilized by an organization, is critical in establishing this type of environment.

A tip is the most common way that organizations detect fraud. The ACFE's *Occupational Fraud: A Report to the Nations* consistently shows that the majority of occupational frauds are uncovered by tips, and approximately half of those tips come from employees. The ACFE surveys also report that about 15% of tips are submitted anonymously. Thus, the percentage of tips originating from employees is likely higher than 50%. Consequently, a whistleblower system is a vital fraud risk management component for any organization that seeks to proactively deter, detect, and address misconduct. It also allows management to identify areas that might need improvement or areas where refresher training might be necessary. In short, a reporting system is one of the most effective approaches to deterring fraud that organizations can implement as part of their Fraud Risk Management Program.

Reported incidents may vary widely in scope, including concerns regarding theft, fraud, corruption, bribery, harassment, violence, cyber-bullying, racial or gender discrimination, concerns about benefits, employment bias, health, and wellbeing. The problems reported can be complex, sensitive, and emotionally challenging, both for those making reports and those responsible for intake. The best reporting processes reduce friction and discomfort so that wrongdoing is more likely to be reported.

The use of a whistleblower system may be required for some organizations. For example, the U.S. Sarbanes-Oxley Act of 2002 requires SEC registrants to establish a reporting mechanism to handle incoming complaints about accounting, internal control, or auditing matters. In addition, the European Union's Whistleblower Directive (Directive (EU) 2019/1937) requires certain companies or public bodies in the EU to implement internal reporting channels and processes, and provide protections to whistleblowers who report violations of EU law.

Like most initiatives, a whistleblower system is most effective when supported by the organization's leadership. Additionally, a senior-level "champion" who owns and oversees the whistleblowing system also reinforces its significance.

Marketing the existence of a whistleblower system to increase awareness, making it easy to use, and ensuring the timely handling of all reported issues are strong preventive controls that supplement the detective control of such reporting systems. Promotion of the system with educational materials provided to shareholders, employees, customers, vendors, the public, and other stakeholders, all of whom can provide valuable information, is an important element of an effective Fraud Risk Management Program. Some organizations have implemented systems that encourage stakeholders to report positive information as well as allegations of wrongdoing, thereby promoting greater awareness of the system and how to utilize it.

Most whistleblower reporting systems traditionally focused on telephone hotlines. The use of email and web-based or online forms, secure anonymous text chat, cloud-based channels, and smartphone apps that enable victims and witnesses to report wrongdoing securely and anonymously are just some of the evolving technologies that are making whistleblower reporting systems more effective and less costly. Consequently, when setting up a whistleblower program, management can provide individuals with every possible means to report misconduct. The objective is to remove all possible barriers to reporting so that a person with a concern will feel free to report it. Ideally, a whistleblower system includes a variety of reporting channels that can be used that provide multilingual support, that are easily accessible and available 24 hours a day, 365 days a year, and that facilitate two-way communication with the reporting party while still maintaining anonymity of those reporting concerns. The inability to have ongoing two-way communications with those wishing to remain anonymous is one of the major shortcomings of telephone reporting systems.

A provision for anonymity for any individual who willingly comes forward to report a suspicion of fraud is a key to encouraging such reporting and an important component of the organization's policy. Whistleblower systems generally preserve the confidentiality of those reporting and provide assurance to employees that they will not be retaliated against for reporting their suspicions of wrongdoing made in good faith — including wrongdoing by their superiors.

In certain jurisdictions, however, anonymous whistleblowing is discouraged and may be subject to restrictions. Additionally, if any of the information used by the whistleblower in filing the complaint was obtained without permission (e.g., classified, confidential, or proprietary), then there may be legal issues in disclosing the information. As such, multinational organizations may not be able to implement such systems on a worldwide basis. To ensure that whistleblower systems comply with all regulations and restrictions, consultation with legal counsel is important. For example, although some countries allow for reporting programs, they may not allow the use of anonymous reporting mechanisms.

Providing whistleblower support is arguably the most important aspect of a whistleblower system; doing so can greatly increase the number of individuals willing to report wrongdoing. Effective management of reporting mechanisms will recognize that whistleblowers face numerous risks — real or perceived — such as ostracism, losing their jobs, losing friends, hurting their professional reputations, and even suffering physical harm.

Therefore, management will commit to fostering an environment where employees feel comfortable escalating concerns. It is beneficial for companies to have a standard approach or procedure once an employee reports a concern. One way to do this is to follow up with employees who did not report anonymously and let them know the outcome of the investigation. A system that allows communications with even anonymous whistleblowers enables all whistleblowers to be informed of outcomes. Whistleblowers want to know that their concerns have been addressed. This shows that management takes whistleblower concerns seriously and eases concerns about potential retaliation. Creating this type of culture within the organization not only reduces management's chance of liability, but also empowers employees to report instances of misconduct.

In any organization, many tips may be without merit, and others will be either intentionally or unintentionally incorrect or misleading. Consequently, the response to reports often determines the overall success of the whistleblower system. In other words, each tip is seriously considered, those with merit are fully investigated, and the whistleblower is kept informed.

A key element of an effective whistleblower system is a well-enforced anti-retaliation policy. The purpose of this policy is to provide employees and third parties with assurance that they can report their concerns about potential misconduct in good faith and without fear of retaliation. For this to work, management will make it clear that there is zero tolerance for retaliation and anyone — no matter their level in the company — will receive disciplinary action if a reported concern turns out to be an act of misconduct or fraud. Furthermore, retaliating against anyone who makes a report in good faith may be a criminal offense. There are numerous laws at the federal and state level in the United States prohibiting retaliation. The European Union's Whistleblowing Directive prohibits covered entities from retaliating against a whistleblower for reporting breaches of the law in a specified list of areas.

An effective whistleblower system will include steps for following up with the person making the report. Following up on each report and providing feedback lets employees know that management is reviewing their concerns, valid or not, and is taking them seriously. It also provides a conduit to obtain additional information from the whistleblower during the course of an investigation. Further, it can empower employees to continue using the reporting program anytime they believe that misconduct has occurred.

An effective whistleblower system will also include mechanisms for formally assessing the system's effectiveness. In doing so, however, management will be aware that a low volume of reports is not the target; in fact, a low number of total reports may indicate employees' discomfort or hesitancy to report, rather than a lack of wrongdoing. Employee surveys are particularly useful in gauging how staff perceive the program.

A single case management system is the optimum method of logging and consolidating all reports and the follow-up actions (regardless of whether they surface through the whistleblower system or other channels). Such a system facilitates management of the resolution process, efficiency in how investigations are conducted, and oversight by the board and the audit committee. In general, the board is responsible for approving protocols to ensure the dissemination of fraud-related issues in a timely manner to appropriate parties, such as the ethics or compliance team, HR, the board or the audit committee, legal, and security. Distributing reports to these parties regarding the occurrences of fraud in their respective areas of responsibility ensures that no single person or functional area controls this highly sensitive information. This distribution also increases accountability.

Organizations placing increased emphasis on their whistleblower reporting systems may find that increased hotline usage results in lower percentages of actionable reports (i.e., potential fraud) as the number of reports increases. Of course, with rigorous follow-up action on reports of potential fraud, the expectation is that the number of actionable reports will diminish over time. It is important for organizations to recognize that an effective reporting system requires a dedication of resources for evaluating and taking action on reports received.

Finally, an important benefit of having a whistleblower system is the ability to analyze and benchmark the data received to identify any trends, increases, or decreases in activity to allow for assessment of underlying root causes. Ongoing analysis allows an organization to continuously refresh its fraud risk assessment and reshape its Fraud Risk Management Program to address new and evolving risks.

Establishes Fraud Investigation and Response Protocols

A "say-something-if-you-see-something" culture that promotes and supports open communication is critical to the achievement of an organization's objectives. It is essential that any reasonably suspected or known violation, deviation, or other breach of the code of conduct, fraud, or corruption be communicated internally and dealt with in a timely and effective manner, regardless of where in the organization these occur or by whom these are committed.

A commitment by the board and senior management to this internal communication process positively encourages the identification of fraud and helps to mitigate the potential risk of retaliation against those who communicate concerns, complaints, or code-of-conduct violations to the organization.

Recognized communication mechanisms within an organization vary and include upward feedback networks, hotlines, dedicated websites, and correspondence to the board or management personnel. The organization reinforces the importance of ensuring that it has a documented process in place to consistently capture, assess, and respond in a timely manner to allegations.

The investigation and response system includes protocols for:

- Updating a central repository for allegations and complaints
- Maintaining anonymity or confidentiality of involved individuals (except as is reasonably necessary to investigate or as required by law or regulation)
- Initially evaluating the allegations to determine if an investigation is warranted and the appropriate degree of urgency
- Considering the impact of data privacy laws or regulations on communication protocols, along with electronic and non-electronic data collection, processing, handling, sharing, and retention activities
- Notifying employees regarding document preservation and securing data systems
- If necessary, engaging independent counsel and forensic accounting support
- Conducting the investigation while controlling and safeguarding evidence

- Reporting the results in the appropriate format (oral summary of key points or comprehensive written report with exhibits)
- Following policies regarding retention of reports, documents, work papers, interview notes, and other information
- Assessing root causes and initiating mitigating processes and controls

Processes for initial triage, safeguarding personnel and operations, organizing an investigation, considering data privacy laws or regulations, securing and gathering evidence, and conducting fact-finding and admission-seeking interviews in a virtual or hybrid work environment are outlined in multiple industry publications, professional online blogs and podcasts, and other published works.

Receiving the Information

Fraud or misconduct allegations may come to the organization's attention in many ways, including tips from employees and former employees, information in resignation letters and exit interviews, and information from customers (e.g., customer service lines) or vendors. Protecting anonymity can be critical, depending on the nature of the allegation and the individuals involved. Fraud allegations also are generated through process control identification, proactive fraud reviews, data analytics, external audits, company surveys, notification by regulators and law enforcement, other mechanisms (such as company websites or social media) where individuals can air concerns, or even by accident. Where internal audits uncover a potential or likely fraud, the findings may be passed to the appropriate internal or external agents to conduct a thorough review.

An organization, through its code of conduct or whistleblower policy, may require an employee or associate to exhaust internal communication structures before revealing information about an alleged fraud or misconduct to third parties, except a law enforcement or regulatory agency. Such a policy may seem to protect the organization, yet it also could have the negative effect of chilling the enthusiasm for reporting allegations of fraud or misconduct. This negative effect occurs particularly when the whistleblower bringing forth the complaint or allegation does not see any meaningful response by management or the board. In those instances, the whistleblower may feel compelled to communicate the complaint to law enforcement, regulators, or the media.

An organization's reporting process is strengthened when the organization acknowledges and communicates appreciation for the employee reporting; invites the sharing of supplemental details about the matter; periodically updates the employee on the status of the organization's efforts to address the allegations and complaints; and advises the employee when the matter has been resolved and, once again, thanks her or him for the input.

The board ensures that the organization develops a system for prompt, competent, and confidential evaluation, investigation, and resolution of allegations and complaints involving potential fraud or misconduct. The board also oversees the response to allegations and complaints relating to senior management.

For organizations required to comply with the Sarbanes-Oxley Act of 2002 (SOX), the system complements procedures established by the board, as referenced in SOX Section 301, "Public Company Audit Committees," for the receipt, retention, and treatment of complaints involving accounting, internal accounting controls, or auditing matters. The board defines clearly and communicates to management the protocols for the board's involvement in such cases, which varies depending on the nature, potential impact, and seniority of persons involved.

The process approved by the board to follow up on allegations or complaints includes a tracking or case management system. In most cases, a member of senior management reviews each allegation unless it affects senior management. In those instances, a designated member of the board reviews the allegations and takes appropriate action.

If the organization has operations in non-U.S. countries, special care is needed when designing the reporting mechanisms for employees, vendors, and third parties. Laws and regulations surrounding privacy vary from country to country and, for example, can restrict the nature of information sought in an investigation. Legal counsel with specific knowledge about the privacy laws of each country in which operations exist is consulted prior to implementing international investigation and reporting mechanisms.

Evaluating the Allegation

Once an allegation is received, the organization follows the documented process approved by the board to evaluate the allegation. A well-designed process includes established criteria for segregating those allegations that are more routine and can be properly handled within the organization from those that are more serious and may require engaging outside counsel and experts.

The process includes designating or retaining an individual or individuals who are free from conflict with the necessary authority and skills to conduct an initial evaluation of

the allegation to determine the appropriate course of action to resolve it. In cases that involve the board or senior management, the board may want to hire outside independent counsel to assist in this evaluation.

Similarly, allegations that suggest larger, more complex, or collusive behavior, or that might implicate the financial reporting function; those that might suggest risk of harm to the public or employees; inquiries by regulators or enforcement authorities; or allegations of illegal conduct by the organization or its representatives might require retention of independent counsel and outside experts. For example, if the potential violation relates to misconduct involving the CEO, the board is notified of the allegation and ensures that the CEO is not involved in, able to influence, or able to oversee the investigation.

Developing Investigation Protocols

Investigations are performed in accordance with protocols approved and documented by the board. Investigation protocols assist the organization in responding to potential fraud and mitigating potential losses promptly. These protocols are referred to as a fraud response plan.

In most instances, those in charge of the organization's overall Fraud Risk Management Program document a formalized fraud response plan outlining how the organization receives, retains, evaluates, investigates, documents, and reports on fraudulent activity. The board reviews and approves this fraud response plan. The fraud response plan also outlines the board's authority to conduct investigations independently of the organization as well as the type of allegations that senior management refers to the board. Further, the fraud response plan outlines the authority of those responsible for conducting internal investigations within the organization and states that those with the authority have unlimited access to all company employees and records for the purpose of conducting an investigation.

Having an approved fraud response plan in place in advance of a matter arising allows the organization to quickly and consistently respond to issues regarding potential losses to the organization. An organization, through its independent investigative team, evaluates each allegation and determines the appropriate **investigative work plan** where merited and feasible.

Each investigation requires an individual with sufficient authority and independence of the matter who is assigned overall responsibility for the investigation. The responsibility for overseeing an investigation resides with an individual with a level of authority at least one level higher than anyone potentially involved in the matter, or with a department that is inherently independent within the organization (such as legal, compliance, security, or internal audit). The board, a designated committee of the board, or an independent member of senior management designated by and reporting to the board oversees investigations of matters involving senior management. Depending on the nature and severity of the allegations, the board or general counsel for the organization may engage outside legal counsel independent of the organization to conduct the investigation.

The designated individual with overall responsibility for the investigation coordinates the investigation and interfaces with management as necessary. That leader clearly communicates the roles and responsibilities of each team member.

Individuals who are competent in the subject matter of the allegation and have sufficient expertise, such as investigation skills, subject matter knowledge, industry expertise, cultural and language fluency, information systems knowledge, and data analytics skills, are identified to perform the investigations. Investigation team members follow applicable professional standards and are free from any conflicts of interest with respect to the issues and individuals under investigation to enable them to conduct an objective assessment. All team members consider whether there is an actual or potential conflict of interest with any of the issues or parties. Should the organization not have adequate internal resources or if the organization determines that internal resources are not sufficiently objective, the organization considers retaining outside expertise.

The team develops a written investigative work plan to guide the investigation and allow for oversight by investigative management. Since investigations are dynamic, they may expand or contract and may require an increase, decrease, or modification of the work plan based on the facts as they are uncovered.

Factors to consider in developing the investigation work plan include:

- **Defined engagement scope** — The engagement scope is sufficient to develop a full understanding of the facts surrounding the allegation. If the allegation is found to have merit, the scope provides reasonable assurance that there are no other instances with similar attributes (e.g., similar problems with the same transaction type, same individual, same accounts, same manager, or same geography).
- **Time sensitivity** — Investigative policy will have timelines established, because an allegation may have a career impact on those accused. Timeliness may be needed due to legal requirements, to enable the organization to mitigate losses or potential harm, or to institute an insurance claim.

- **Notification** — Certain events may require timely notification to regulators, law enforcement, insurers, external auditors, or legislative oversight committees.
- **Confidentiality** — Information gathered is kept confidential, and distribution is limited to those with an established need to know.
- **Legal privileges** — Involving legal counsel early in the process or, in some cases, involving legal counsel to lead the investigation helps safeguard work product and attorney-client communications.
- **Compliance** — The investigation team complies with applicable laws and rules regarding gathering information, transmitting electronic data, conducting workplace surveillance, interviewing witnesses, and recording investigation meetings and discussions.
- **Secure evidence** — The investigation team protects the **chain of custody** of all evidence gathered to ensure that it is not destroyed and that it is admissible in legal proceedings.
- **Goals** — Specific issues or concerns appropriately influence the focus, scope, and timing of the investigation.

When conducting an international investigation, the investigation team considers the laws and regulations of the country (and the local territory within the country), customary business practices, the native language and potential communications barriers, transportation, and other logistics. If required knowledge regarding the international investigation does not exist internally within the organization, the investigation team, with approval from internal legal counsel, seeks the assistance of third-party subject matter experts in the development of the investigation plan.

When it is advisable to engage independent outside counsel to conduct the investigation, that counsel then engages other experts as necessary. These experts could come from within or outside the company. Internal personnel, while not independent, may be assigned to work on investigations to the extent that they are competent and objective. In complex, higher-risk investigations, it is common to rely on independent, external resources to enhance the credibility and reliability of the investigation when viewed by regulators and external auditors. Depending on the specifics of the matter under investigation, the investigation team may reach out to subject matter experts for assistance. Subject matter experts can include computer forensic specialists, forensic accountants, and those with specific industry skill sets.

Conducts Investigations

Investigations are conducted with integrity and objectivity. Investigations performed by certified public accountants (CPAs) adhere to the AICPA *Code of Professional Conduct* and comply with the AICPA *Statement on Standards for Forensic Services No. 1*. Similarly, investigations performed by Certified Fraud Examiners adhere to the ACFE *Code of Professional Ethics* and the *CFE Code of Professional Standards*. All work conducted by Certified Internal Auditors, that may be subsequently used to inform a fraud investigation, adheres to The Institute of Internal Auditors' *Code of Ethics*.

Government regulators and enforcement authorities follow the relevant statutory and regulatory guidance applicable to their jurisdiction. Investigations conducted by federal government inspectors general follow *Quality Standards for Investigations* issued by the Council of the Inspectors General on Integrity and Efficiency, federal rules of evidence, and Attorney General Guidelines. U.S. federal law enforcement authorities also follow the federal rules of evidence, among other things.

Dynamic changes in the nature and composition of the global workforce, mobility programs, and adoption of innovative new technologies have a substantive and continuing impact on the manner in which investigations are conducted. Multiple publications available through the AICPA, IIA, and ACFE, as well as professional online blogs and podcasts, address evolving investigation processes for remote and hybrid work environments.

The AICPA publication, *Forensic Accounting – Fraud Investigations*, contains more detailed information on conducting investigations. The publication explains the types of engagements a practitioner may be asked to perform, and provides helpful guidance on engagement acceptance, performance, reporting, and deliverables (including testimony).

Having a documented plan is essential to a thorough and competent investigation. The investigation team establishes the investigation tasks as outlined in the investigation work plan and assigns each task to the appropriate team members. The plan prioritizes the performance of tasks to provide an interim report of findings, if necessary, and to revise or plan next steps.

At this stage, the investigation team considers legal issues and constraints in dealing with employees and third parties, obtains relevant information, and develops related

documentation. This effort may include seeking assistance from the courts and monitoring the integrity of the results of the investigation to ensure that results remain viable for subsequent prosecution efforts, thereby maximizing the prospects of success.

The investigation team may modify the work plan as the investigation proceeds to increase, decrease, or modify the investigation's scope and tasks based on facts as they are uncovered.

Investigations generally include many of the following procedures:

- Gathering evidence and performing analysis, including:
  - Reviewing and categorizing information collected
  - Performing computer-assisted data analysis
  - Developing and testing hypotheses
- Gathering external records from public sources, customers, vendors, and others, including social media, news media, and industry reports
- Examining computer forensics to collect evidence from internal sources consisting of hard copy and electronically stored information residing in servers, computers, personal and company phones, printers, and other devices; building access logs and physical security cameras, and IT system records in spite of their short retention period
- Interviewing witnesses, usually starting with peripheral witnesses and proceeding to the target or subject of the investigation

The investigation team documents and tracks the information related to the steps of the investigation, including:

- Items maintained as privileged or confidential
- Requests for documents, electronic data, and other information
- Memoranda of interviews conducted
- Analyses of documents, data, and interviews and conclusions drawn

This documentation and tracking allow the team to control the information relevant to the investigation and allows, for quality control and investigative supervision. These documents are also critical to protecting against investigative misconduct.

If, during the investigation, the allegations are substantiated or appear as if they are likely to have occurred, the investigation team evaluates the root cause of the issues during the course of the investigation (e.g., by asking, "Is this a systemic or recurring issue?" "What behavioral red flags did the perpetrator exhibit?" "What weaknesses did the perpetrator exploit?" and "Why did the perpetrator believe detection could be avoided?"). This evaluation can affect the individuals that are interviewed, the questions that are asked during the interviews, and the scope of the investigative procedures. Identifying the root cause of the issue is valuable information to the organization and assists the investigation team in its resulting development of recommendations to senior management to prevent similar issues from occurring in the future.

Performs Data Analytics

The objective of data analytics in support of the investigation of potential fraud is to analyze entire populations of transactional data, master data, and **application control** settings to look for indicators to negate or support an allegation. Analytics also assist in identifying the full scope of potential financial impact. Reliance on tests of samples of data is generally insufficient for finding warning patterns, and is often inadequate to fulfill regulatory and evidential needs. Detailed data analysis provides insights into the effectiveness of internal controls and identification of indicators of wrongdoing. Data analysis technology can assist in identifying fraud risks and control weaknesses within an organization, and in focusing the investigations of potential fraud.

The development of a data analytics plan will be considered to support the fraud investigation. Such a plan includes, at a minimum, types and format of data available to the investigation team, data locations, analytic procedures, timelines, and deliverables. The data analytics plan will include steps to identify and protect required data; develop, test, and verify analytics to support the investigation; and allow for ongoing monitoring of high fraud-risk areas.

In cases of suspected fraud, the data used in the analysis is verified to the source or system of record to confirm completeness and accuracy. This may also include the comparison with other sources or financial records, such as a trial balance. When performing the analysis, often the data will be analyzed at the transactional level. When applying professional skepticism, the assumptions and results are evaluated for bias.

Example Data Analytic Tests

To assist organizations in getting started with integrating data analytics into their investigative work plans or a fraud risk assessment as identified in Chapter 2, a library of test examples is posted to the COSO web site for reference located at ACFE.com/fraudrisktools. These tests are organized by asset misappropriation, corruption, and financial misstatement classification categories and provide general guidance and examples for consideration in forensic data analytics efforts.

Communicates Investigation Results

Reports of an investigation prepared by a third party (e.g., outside legal counsel) engaged to conduct the investigation are delivered to the official within the organization that engaged the services of the third party (e.g., general counsel, CEO, board chair, or board committee chair). Reports prepared by third-party subject matter experts engaged to review or investigate aspects of the allegations are delivered to the lead investigator for use in preparing the final report of investigation.

Reports of investigation prepared by the organization's internal investigators are delivered to the individuals within the organization overseeing the investigation (e.g., legal counsel, senior management, or directors) who ultimately will decide on the specific disciplinary and other actions to be taken.

The investigation report is accurate, clear, objective, and impartial. It is timely in its preparation and delivery.

The investigation report presents only the relevant facts and the evidence that has been gathered and any summaries or analyses that are helpful for decision-makers. Generally, investigation reports do not include an ultimate conclusion regarding whether fraud has occurred. Since the determination of whether fraud occurred is ultimately a legal decision, this conclusion is left to judges, juries, and other triers of fact.

Elements of an investigation report may include:

- Executive summary
- Background information on the matter under investigation
- Investigation procedures performed
- Evidenced-based findings and recommendations, which may include recommendations for remediation
- Appendices or exhibits

The nature and distribution of the report may depend on the goals of protecting attorney-client and attorney work product legal privileges and avoiding risks arising from defamatory statements or retaliation. For similar reasons, obtaining advice of legal counsel before the party overseeing the investigation makes public statements or other communications regarding the investigation is warranted.

Generally, investigation work products are kept confidential. Those with overall responsibility for the investigation may choose to disclose some aspects of the investigations. For example, disclosure could be made as part of a public announcement, as part of internal communications regarding the fraud risk program, as a message related to process improvement, or to law enforcement or regulatory bodies.

At the conclusion of the investigation, the investigation team may discuss the results with individuals who provided information to the organization. Information shared with these individuals varies on a case-by-case basis, and the investigation team reinforces the confidential nature of the information. The investigation team also may seek feedback about whether these individuals believe that the matter was dealt with reasonably, objectively, and appropriately.

As discussed in Chapter 3, one of the most effective fraud deterrents is an organizational culture that clearly communicates to its members through its words and actions that anyone attempting to commit fraud faces a high likelihood of getting caught and being held responsible and punished. Consequently, communication of the results of investigations to others in the organization enhances fraud deterrence.

Takes Corrective Action

After the investigation is completed, the organization determines what action to take in response to the findings. The investigation team may report any significant (more than inconsequential) findings of actual or potential material impact to the board, the audit committee, and to both the internal auditor and external auditor if they are not receiving investigation reports directly. It also may be necessary to notify the public, law enforcement, regulatory agencies, legislative oversight committees, and the organization's insurers.

The organization will consider the possibility that a similar fraud may be occurring elsewhere in the organization — taking advantage of the same or similar fraud risks and control weaknesses. Often, data analytics can be used to determine if this is the case. The information may also be used to refresh scenarios considered during the fraud risk assessment process.

Any action taken is appropriate in the circumstances, applied consistently to all levels of employees (including senior management), and taken only after consultation with individuals responsible for such decisions. Remediation that addresses training, business processes, and internal control deficiencies is directed to an appropriate level of management. The board is advised of the nature, timing, and status of the remediation plans. The internal audit function is well positioned to monitor remediation and report to senior management and the board.

The investigation team makes a report to the board or to the appropriate internal sponsor of the investigation about the remediation of issues related to training, business processes, and internal control deficiencies. Management consultation with legal counsel is recommended before taking disciplinary, civil, or criminal action.

Among the possible corrective actions that the organization may take are:

- **Internal control remediation** — The organization may wish to enhance certain internal controls to reduce the risk of similar frauds or misconduct going undetected in the future.
- **Business process remediation** — The organization may be able to re-engineer its business processes cost-effectively to reduce or remove the opportunity for similar frauds or misconduct in the future.
- **Disciplinary action** — The organization may take internal disciplinary action, which may include termination, suspension (with or without pay), demotion, or warnings.
- **Training** — The organization may need to provide education about its policies and procedures to enhance awareness of ethical business practices or requirements.
- **Insurance claim** — The organization may be able to pursue an insurance claim for some or all of its losses.
- **Root cause analysis** — The organization may conduct a formal root cause analysis and perform additional procedures to ensure remediation is addressing the most probable root cause(s), if not already identified and confirmed during an investigation. Root cause analysis may also help identify similar misconduct occurring elsewhere in the organization.
- **Civil action** — The organization may pursue its own civil action against the perpetrators to recover lost assets and investigation expenses.
- **Criminal referral** — The organization may refer the case to law enforcement voluntarily, and, in some cases, may be required to do so. Law enforcement has access to additional information and resources that may aid the case. Additionally, referrals for criminal prosecution may increase the deterrent effect of the organization's fraud prevention policy. The decision to make a criminal referral is a serious one and can have repercussions. A referral that does not lead to a prosecution and conviction may enable the target to sue the organization and the individual professionals involved in the investigation and reporting. Therefore, an appropriate member of senior management, such as the chief legal counsel, is authorized to make the decision as to whether pursuing criminal prosecution is appropriate.

The nature and extent of an organization's corrective actions depend on specific facts and circumstances, including the nature of the investigation findings. A strong, clear, and consistent response that embodies the values of the organization and good corporate conduct reinforces the Fraud Risk Management Program. A strong response also sends a positive message to external stakeholders, such as the public, the company's regulators, and the company's investors, even when the investigation has uncovered improprieties.

Evaluates Investigation Performance

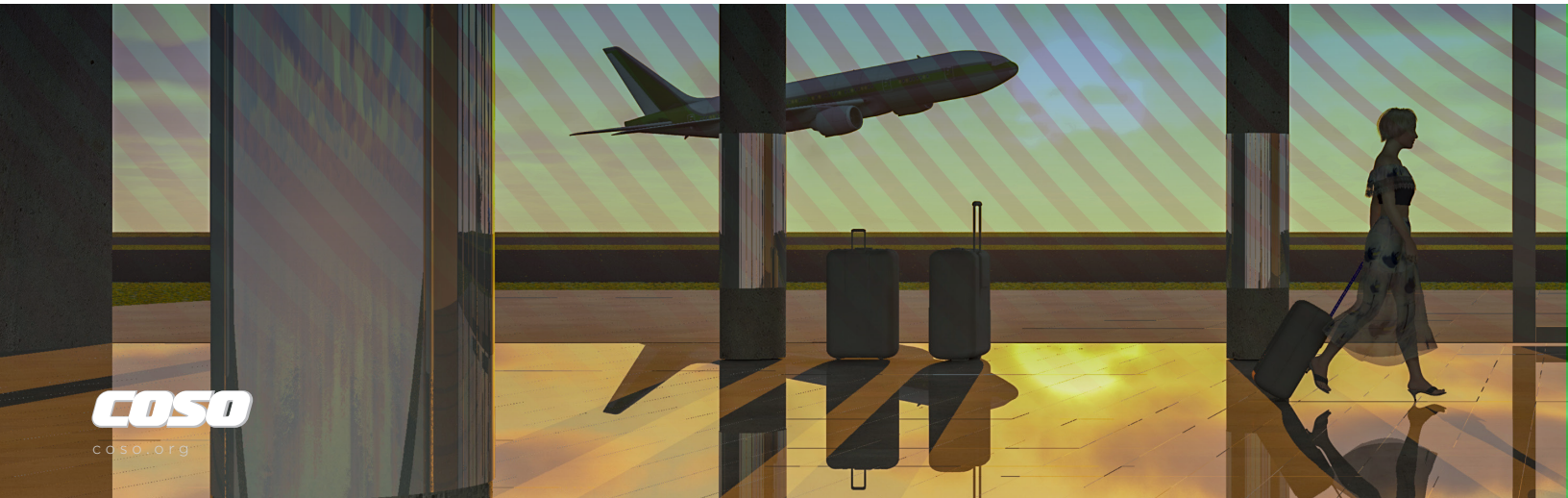
The scope, scale, and complexity of fraud investigations can vary considerably. Therefore, such investigations require some flexibility or customization for the performance metrics adopted by the organization to evaluate the efficiency and effectiveness of the investigation process.

Although it is possible to apply a variety of performance metrics, the following metrics may be relatively simple and beneficial to monitor:

- **Resolution time (average number of days to resolve an issue)** — Time spent on investigations can be measured separately for different categories of incident to avoid creating pressure to resolve complex cases in an unrealistically short time.
- **Investigation cost (resource hours and external spending)** — The amount of resource time incurred on investigations can help inform the organization's investment in resource management, training, and tools (such as data analytics, case management software, and computer forensic equipment). Organizations can use external service provider fees for budget planning purposes and negotiating future arrangements.
- **Repeat incidents (number of current-period incidents that are similar in nature to incidents in earlier periods)** — A low rate of repeat incidents can demonstrate effectiveness in promptly and comprehensively remedying business processes and internal controls in response to earlier incidents.
- **Incident location (number of incidents in a specific business unit, operational area, or geography)** — A pattern of incidents at a certain location may indicate a systemic management issue or weakness in the organization's internal control framework that may require additional attention.
- **Value of losses recovered and future losses prevented** — Fraud investigations are important for their deterrent effect, so judging their cost-effectiveness only by the assets they help to recover (cash or assets) is not sufficient. Pursuing asset recoveries vigorously and estimating future losses prevented can help demonstrate the value of fraud risk management actions.
- **Corrective actions (type of remediation and implementation date)** — The type of action taken as a result of an investigation, as well as the completion time for remedial activity, can help the organization better assess the impact of fraud investigations in achieving its business objectives.

As discussed in Chapter 5, each person responsible for fraud risk management principles communicates promptly, through the appropriate channels, details of any modifications necessary or any fraud risk management processes that no longer assist in reducing residual fraud risk to an acceptable level in accordance with the organization's risk tolerance. The information and communications required for fraud investigations and corrective actions are critical elements in this ongoing evaluation.

Once the organization has established procedures to conduct initial and follow-up fraud risk assessments, designed and implemented appropriate fraud control activities, and established fraud investigation and corrective action systems, the final phase of the fraud risk management process is implementation of a system for monitoring the effectiveness of the entire fraud risk management process and each of its component principles. Chapter 5 explains this last important aspect of fraud risk management.



CHAPTER 5. FRAUD RISK MANAGEMENT MONITORING ACTIVITIES

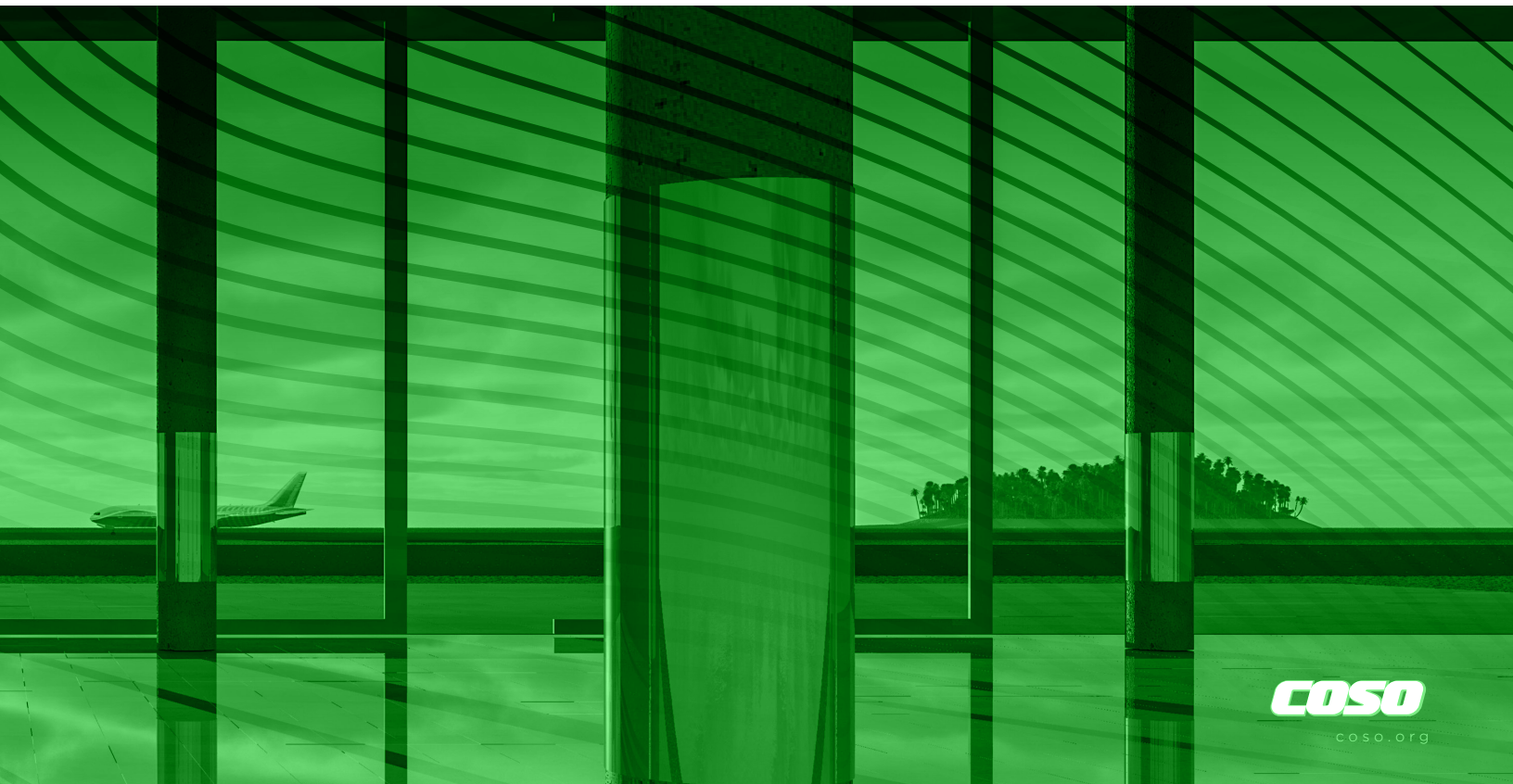
Chapter Summary

The first four fraud risk management principles relate to fraud governance, fraud risk assessment, fraud prevention and detection control activities, and fraud investigation and corrective action. The fifth fraud risk management principle relates to monitoring the overall Fraud Risk Management Program. Organizations use Fraud Risk Management Program 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. This chapter explains these monitoring activities.

Organizations use ongoing and 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 feedback and information that may be used to re-evaluate fraud risk. 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 assist the organization in continuously improving its Fraud Risk Management Program. For example, these activities provide input for continuous corrective action. If the monitoring activities identify deficiencies, organizational leadership oversees the timely improvement and correction of those deficiencies according to its follow-up plan.
Part of this monitoring activity includes assessment and periodic reassessment of each principle in the Fraud Risk Management Program. ACFE's Fraud Risk Management Tools web site (ACFE.com/fraudrisktools) has five fraud risk management scorecards that can be used in performing assessments of each of the five fraud risk management principles to aid in determining how comprehensive an organization's Fraud Risk Management Program is and how well it is achieving its objectives.

Further, an ongoing evaluation of the implemented Fraud Risk Management Program includes conducting overall evaluations of the organization's policies and procedures for fraud risk management. The ongoing evaluation focuses on the design of the Fraud Risk Management Program and is an important monitoring activity that is integral to the overall evaluations considered in this chapter.



Fraud Risk Management Monitoring Activity Principle

This chapter addresses Principle 5 of a Fraud Risk Management Program. Principle 5 states:

Chapter introduces **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.

Relationship to the COSO 2013 Internal Control Framework

In addition to the requirement to assess fraud risk in the COSO 2013 IC Framework Principle 8 (*The organization considers the potential for fraud in assessing risks to the achievement of objectives*), each component and principle of the COSO 2013 IC Framework is relevant to the consideration of the risk of fraud. Therefore, the principle discussed in this chapter about Fraud Risk Management Program monitoring activities mirrors the COSO 2013 IC Framework's monitoring activities' principles. The COSO 2013 IC Framework, when read in conjunction with this chapter on fraud monitoring activities, provides informative context regarding the topic of this chapter.

Fraud Risk Management Principle 5 correlates with the COSO 2013 IC Framework's monitoring component and principles as follows:

Figure 17. Fraud Risk Management Principle 5 Correlates with the COSO 2013 IC Framework's Components and Principles

COSO Framework Components and Principles		Fraud Risk Management Principle
Monitoring Activities	**16.** The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**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.
	17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	

While the COSO 2013 IC Framework's monitoring activities principles are broadly designed to help ensure that each component of internal control is present and functioning as designed, Fraud Risk Management Principle 5 focuses specifically on ensuring that each principle of the Fraud Risk Management Program is present, functioning, and operating in an integrated manner.

Points of Focus

The following points of focus highlight important characteristics relating to this principle:

- **Considers a Mix of Ongoing and Separate Evaluations —** Management includes a combination of ongoing and separate Fraud Risk Management Program monitoring evaluations to determine whether each of the five principles of fraud risk management is present and functioning.
- **Considers Factors for Setting the Scope and Frequency of Evaluations —** Management considers changes in the organization, its operating environment, and its control structure to determine the appropriate scope and frequency of its Fraud Risk Management Program monitoring activities.
- **Establishes Appropriate Measurement Criteria —** Management establishes appropriate measurement criteria to assist in the objective evaluation of its Fraud Risk Management Program.
- **Coordinates with Other Risk- and Compliance-Focused Functions in the Business —** Management coordinates the assessment and monitoring of the Fraud Risk Management Program with other functions throughout the business and ensures alignment of the program with legal and regulatory requirements.
- **Considers Known Fraud Schemes and New Fraud Cases —** Management considers known fraud schemes and newly discovered or reported frauds in other organizations and assesses the likelihood of occurrence in the organization.
- **Evaluates, Communicates, and Remediates Deficiencies —** Management and the board of directors assess the results of ongoing and separate Fraud Risk Management Program monitoring evaluations, communicate deficiencies to those responsible for corrective action, and determine that appropriate remediation is implemented in a timely manner.
- **Uses Data Analytics to Continuously Monitor and Improve —** Management understands that the application of data analysis techniques, including continuous monitoring, can usually be an effective way to ensure that the fraud risk policies and procedures discussed in Principles 1 through 4 are being adhered to on an ongoing basis.

Considers a Mix of Ongoing and Separate Evaluations

Ongoing evaluations are generally routine processes that monitor a control activity on a real-time basis. A fraud risk management monitoring plan that targets the organization's areas of highest fraud risk assists the organization in managing an ongoing evaluation of the five principles of fraud risk management.

Whether an activity is classified as a control activity or a monitoring activity is a matter of judgment. Generally, a monitoring activity focuses on these aspects of the analysis performed: "why," "who," what," "where," and "what's next"? Ongoing monitoring activities may include data analytics. Figure 18 illustrates the subtle distinction between control activities and monitoring activities.

Separate periodic evaluations help assure management that the organization's Fraud Risk Management Program is functioning as designed. Internal audit, others within the organization, or third parties can perform these separate periodic evaluations.

The organization documents its plan, approach, and scope for monitoring its Fraud Risk Management Program. The plan includes the balance of ongoing and separate evaluations deemed appropriate to assist management in its evaluation of whether each of the five principles of fraud risk management is present and functioning in its Fraud Risk Management Program. Significant changes in the organization or in its operating environment that increase or change the risk of fraud warrant making changes to the overall Fraud Risk Management Program.

Figure 18. Interrelationship between Fraud Risks, Control Activities, and Monitoring

Fraud Risk
An employee could declare inventory as "not repairable," authorize a write-off of the inventory as scrap, and take or otherwise misappropriate those inventory items.

Related Fraud Control Activity
The fraud risk is mitigated by a separation of duties such that the same person is not authorized to both designate inventory as "not repairable" and initiate inventory write-offs.

Ongoing Monitoring Plan Using Data Analysis
Identify all employees who designated inventory as "not repairable" and those who initiated write-offs of inventory. Generate an automatic error report if employees are on both lists. Assign an inventory supervisor the responsibility to investigate the results weekly and evaluate and communicate any internal control deficiency to those in the inventory processing area who are responsible for taking corrective action.

While these activities may be considered detective control activities, they also provide the information necessary to monitor these control activities. For example, management, independent of the control activity, determines whether exception report results are appropriately produced, reviewed, and communicated. In addition, there is assessment of the competence of personnel performing the review as well as root causes for the segregation of duties not operating properly.

Considers Factors for Setting the Scope and Frequency of Evaluations

Before performing each evaluation, or periodically, management considers the factors affecting the scope of ongoing and separate evaluations. Based on the outcome of the assessment, management may alter the scope of the evaluations.

For most organizations, it is reasonable to expect that fraud risks are constantly changing over time, as do the industry and business environments in which the organization operates. For example, the impacts the COVID-19 pandemic had on remote working and the global supply chain were profound. For most companies, fraud risk assessments conducted in mid-to-late 2019 were likely outdated by the Spring and Summer of 2020 given how fast the pandemic spread and how quickly organizations had to adapt. From a data analytics perspective, analyzing data taking a periodic, lookback approach is simply not as effective as continuously monitoring for anomalies and trends on a proactive basis.

The US Department of Justice's guidance to government enforcement authorities provides insight on its expectations for corporate anti-fraud and regulatory compliance programs. Sources for this guidance include its *Evaluation of Corporate Compliance Programs*, public speeches and summaries of recent settlement undertakings. Enforcement authorities continue to expect more rigorous programs with more explicit evaluation of their efficacy. Recent guidance has asked, "Is the periodic review (of a company's risk assessment) limited to a 'snapshot' in time or based on continuous access to operational data and information across functions?" It has also asked "Does the company have a process for tracking and incorporating into its periodic risk assessment lessons learned either from the company's own prior issues or from those of other companies operating in the same industry and/or geographic region?" Recent updates to enforcement guidance indicate an increasing focus by authorities on the use of data analytics to monitor and improve the Fraud Risk Management Program.

Establishes Appropriate Measurement Criteria

In addition to ongoing and periodic evaluations, the organization establishes measurement criteria to monitor and improve fraud prevention and detection and provides the criteria to the organization's leadership on an ongoing basis. For example, measurement criteria may include:

- Number of fraud schemes, e.g., known fraud schemes committed against the organization, fraud allegations received requiring investigation, and fraud investigations resolved

- Length of time to detection of fraudulent activity
- Extent of the loss
- Number of fraud allegations received via the organization's hotline or other means
- Number of employees who have or have not signed the corporate ethics statement or completed ethics training sponsored by the organization
- Number of interactions with employees and stakeholders, e.g., messages supporting ethical behavior delivered by executives and surveys concerning the integrity or culture of the organization
- Number or percentage of vendors and customers who have or have not signed the organization's ethical behavior requirements
- Number or percentage of employees with background checks performed and the number of problems identified in background checks

Organizations also use benchmarks from global fraud surveys and studies of fraud and regulatory compliance to assist in determining the appropriate measurement criteria. Such information can include the type of fraud experienced and average losses. In addition, resources dedicated by the organization to fraud risk management are another useful metric for board consideration.

Once management identifies the appropriate measurement criteria, the manner in which it uses these criteria (e.g., the analytical comparisons) become important to the evaluation. These analyses vary by organization based on factors such as controls in place, fraud risks identified, and resources available. They may include the following:

- Comparison of number of frauds identified versus the complaints, grievances, etc., received via whistleblower reports
- Comparison of frauds identified versus types of frauds previously uncovered
- Comparison of the number of frauds discovered versus the number of fraud investigations performed
- Ratios of problems revealed in background checks versus the number of checks performed

Other metrics about the control environment and the timeliness of implementing remediation plans and additional controls in response to residual risk or identified frauds depend on the complexity of the organization and its control environment.

Coordinates with Other Risk- and Compliance-Focused Functions in the Business

Because a holistic Fraud Risk Management Program touches nearly every part of the organization in some way, it will necessarily overlap with various enterprise-wide initiatives, such as the compliance program and other risk management functions. These overlaps can reinforce the effectiveness of each of the initiatives, as long as any gaps that might enable risks to go unaddressed are minimized. Internal audit is charged with providing independent and objective assurance on the internal control system, while a (sometimes separate) compliance function is charged with preventing, detecting, and addressing legal and regulatory violations. Certain components of these efforts are also part of the objectives of fraud risk management. Consequently, those charged with overseeing the Fraud Risk Management Program coordinate and collaborate with internal audit, compliance, risk management, corporate security, ethics, and other functions as needed to be effective.

As part of this coordination, the Fraud Risk Management Program considers prominent compliance-focused guidance to ensure that the program aligns with relevant legal and regulatory requirements. Examples of such guidance include:

- The *U.S. Sentencing Guidelines for Organizations*, which provide seven elements of compliance programs that will be assessed when determining the potential fines for organizations convicted of wrongdoing
- The U.S. DOJ guidance such as its *Evaluation of Corporate Compliance Programs*, which outlines the questions and metrics the U.S. DOJ uses to evaluate organizations' compliance programs when deciding whether to criminally charge a company or how to resolve criminal charges
- U.S. DOJ and SEC Resource Guides to the *U.S. Foreign Corrupt Practices Act*

- COSO's guidance, such as its *Compliance Risk Management*, which applies the concepts of the COSO Enterprise Risk Management Framework to compliance risk management efforts

Many of the factors and elements covered in these sources of guidance reinforce the principles and points of focus for a comprehensive Fraud Risk Management Program. Considering all of the organization's risk- and compliance-focused initiatives together, as well as through the lens of applicable leading practices and regulatory guidance, can help management ensure that these functions are operating efficiently and effectively to comprehensively protect the organization from harm.

Considers Known Fraud Schemes and New Fraud Cases

It is beneficial to consider known fraud schemes and new frauds discovered within and outside of an organization's industry. When such frauds are uncovered and reported, management reviews its most recent fraud risk assessment and existing control activities to ascertain whether they would be prevented or detected in the organization if they are attempted or occur.

Closely monitoring emerging fraud cases and assuring that the organization is protected against such frauds ensures that the organization's Fraud Risk Management Program remains current in the face of evolving fraud risks. In addition, industry information and benchmarks may provide sufficient information to assist management in an assessment of the likelihood that existing fraud schemes perpetrated against other organizations in the same industry will occur.

Evaluates, Communicates, and Remediates Deficiencies

Senior management and the board of directors assess the results of ongoing and separate evaluations. Those responsible for taking corrective action, senior management, and the board of directors receive communications about identified deficiencies in the Fraud Risk Management Program. Management tracks whether the deficiencies in the Fraud Risk Management Program are remediated on a timely basis and takes further action if necessary.

A senior member of management will be assigned overall responsibility for the Fraud Risk Management Program. In addition, the fraud risk management principles and related fraud control activities can be individually assigned to other senior members of management.

Each person responsible for fraud risk management principles and related fraud control activities:

- Evaluates regularly whether the fraud risk management principles and their related fraud control activities are present and functioning
- Modifies fraud risk management processes and related fraud control activities as required and documents any necessary modifications
- Reports promptly, through the appropriate channels, details of and seeks approval for any modifications necessary or any fraud risk management processes and related fraud control activities that no longer assist in reducing residual fraud risk to an acceptable level in accordance with the organization's risk tolerance

Each evaluation includes evidence that management is actively retaining responsibility for oversight of the Fraud Risk Management Program, taking timely and sufficient corrective measures with respect to any previously noted program deficiencies or weaknesses, and ensuring that the plan for monitoring the Fraud Risk Management Program continues to be adequate for its ongoing success.

Uses Data Analytics to Continuously Monitor and Improve

Data analytics support all aspects of the process of monitoring the functioning of the Fraud Risk Management Program. For example, some organizations accumulate information regarding the expected or benchmark results on the key measurement criteria and the actual results on a periodic basis. This information can be assembled in dashboard reports that provide information on the historic and near real-time information about the performance of the program.

When business is changing rapidly, historical data and comparisons to expected benchmarks or static fraud risk assessments may be less valuable. Fraud risks are constantly changing over time, as are the industry and business environments in which the organization operates. For example, fraud risk assessments conducted prior to 2020 were likely outdated when the global pandemic created rapid change in business processes and supply chains.

Ideally, data analytics that support the monitoring of Fraud Risk Management Programs are not limited to mere snapshots of historical data. Incorporating continuous monitoring of operations and information across functions enables more robust and timely assessments of risks in changing environments. Similarly, monitoring processes and monitoring-related data analytics are more effective when they incorporate lessons learned from either the company's own situation or events or those of similarly situated organizations or those in similar geographic regions.

As discussed further in Appendix D, advances in automation, data gathering, and business intelligence tools have made using data analytics on a continuous monitoring basis more cost-effective and attainable. Waiting to analyze transaction data on an annual basis is no longer a leading practice. Rather, having a dashboard that allows continuous transaction monitoring on a real-time or near real-time basis detects anomalies, errors, or abuses much more quickly, thereby minimizing losses and maximizing deterrence.

Further, when anomalous transactions or events are identified, either through data analytics activities or via other channels such as the fraud risk hotline, the risk triggers and lessons learned from those events can be used to improve the continuous monitoring model. Data analytics techniques such as machine learning and artificial intelligence that incorporate patterns and trends from historical transactions to help identify statistically similar, new transactions are ideal for demonstrating that the Fraud Risk Management Program is continuously improving by incorporating those lessons learned from past events. See Appendix D-3 for further discussion of these techniques.

Forward-thinking and cutting-edge organizations recognize the importance of comprehensive fraud risk management as a key component of both enterprise risk management and the integrated internal control framework. The five principles and supporting points of focus in this guide serve as leading practice policies, procedures, and processes for ensuring that the organization is managing fraud risk effectively.

APPENDIX A

Glossary

Anti-Competitive Practices	Practices "that are likely to reduce competition and lead to higher prices, reduced quality or levels of service, or less innovation. Anti-competitive practices include activities like price fixing, group boycotts, and exclusionary exclusive dealing contracts or trade association rules, and are generally grouped into two types: agreements between competitors also referred to as horizontal conduct and monopolization, also referred to as single firm conduct. The FTC generally pursues anticompetitive conduct as violations of Section 5 of the Federal Trade Commission Act, which bans 'unfair methods of competition' and 'unfair or deceptive acts or practices.'" [Source: Federal Trade Commission]
Application Controls	Programmed procedures in application software and related manual procedures designed to help ensure the completeness and accuracy of information processing. [Source: COSO 2013 IC Framework]
Asset Misappropriation	Misappropriation of assets involves the theft of an entity's assets and is often perpetrated by employees in relatively small and immaterial amounts. However, it can also involve management, who is usually better able to disguise or conceal misappropriations in ways that are difficult to detect. Misappropriation of assets can be accomplished in a variety of ways including the following: • Embezzling receipts (for example, misappropriating collections on accounts receivable or diverting receipts from written-off accounts to personal bank accounts) • Stealing physical assets or intellectual property (for example, stealing inventory for personal use or for sale, stealing scrap for resale, or colluding with a competitor by disclosing technological data in return for payment) • Causing an entity to pay for goods and services not received (for example, payments to fictitious vendors, kickbacks paid by vendors to the entity's purchasing agents in return for approving payment at inflated prices, or payments to fictitious employees) • Using an entity's assets for personal use (for example, using the entity's assets as collateral for a personal loan or a loan to a related party) Misappropriation of assets is often accompanied by false or misleading records or documents in order to conceal the fact that the assets are missing or have been pledged without proper authorization. [Source: Paragraph .11 of AU-C sec. 240, *Consideration of Fraud in a Financial Statement Audit*]
Chain of Custody	A process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer. [Source: National Institute of Standards and Technology]
Channel Stuffing	A deceptive business practice used by a company to inflate its sales and earnings figures by deliberately sending retailers along its distribution channel more products than they are able to sell to the public. [Source: Investopedia]
Collusion	A secret agreement between two or more parties for fraud or deceit. [Source: AIS Auditing Dictionary of Terms]
Control Activity	An action established through policies and procedures that helps ensure that management's directives to mitigate risks to the achievement of objectives are carried out. [Source: COSO 2013 IC Framework]
Control Environment	The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements: • Integrity and ethical values • Management's philosophy and operating style • Organizational structure • Assignment of authority and responsibility • Human resource policies and practices • Competence of personnel [Source: Institute of Internal Auditors, *Standards and Guidance*]
Cookie Jar Reserves	The term "cookie jar reserves" refers to inflated or wholly improper reserves posted to provide a cushion against earnings shortfalls in later periods, when those reserves can be drawn into income. [Source: 33-7976 (sec.gov)]
Corporate Governance	The system of rules, practices, and processes by which a company is directed and controlled. Corporate governance essentially involves balancing the interests of the many stakeholders in a company — these include its shareholders, management, customers, suppliers, government, and the community. [Source: Investopedia]
Corruption	The abuse of entrusted power for private gain. [Source: Transparency International]
Corruption Perceptions Index	The CPI ranks 180 countries and territories around the world by their perceived levels of public sector corruption. The results are given on a scale of 0 (highly corrupt) to 100 (very clean). [Source: Transparency International]
Data Analytics	Data analytics is the science of analyzing raw data to make conclusions about that information. Many of the techniques and processes of data analytics have been automated into mechanical processes and algorithms that work over raw data for human consumption. [Source: Investopedia]
Data Stratification	The process of dividing a population into subpopulations, each of which is a group of sampling units that have similar characteristics. [Source: AU-C Section 530, *Audit Sampling*]
Data Visualization	The presentation of data in a pictorial or graphical format. [Source: SAS]
Enterprise Risk Management	The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value. [Source: COSO 2017 ERM Framework]
False Claims Act	The False Claims Act provides, in pertinent part, that: • Any person who (1) knowingly presents, or causes to be presented, to an officer or employee of the United States Government or a member of the Armed Forces of the United States a false or fraudulent claim for payment or approval; (2) knowingly makes, uses, or causes to be made or used, a false record or statement to get a false or fraudulent claim paid or approved by the Government; (3) conspires to defraud the Government by getting a false or fraudulent claim paid or approved by the Government;. . . or (7) knowingly makes, uses, or causes to be made or used, a false record or statement to conceal, avoid, or decrease an obligation to pay or transmit money or property to the Government. • Is liable to the United States Government for a civil penalty of not less than $5,000 and not more than $10,000, plus 3 times the amount of damages which the Government sustains because of the act of that person. [Source: 31 U.S. Code § 3729 - False claims]

Glossary

Financial Restatement	The process of revising previously issued financial statements to reflect the correction of an error in those financial statements. [Source: FASB Accounting Standards Codification, Master Glossary]
Fraud Control Activity	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 to either prevent fraud from occurring or to detect existing fraud quickly in the event that it occurs. [Adapted from the COSO 2013 IC Framework]
Fraud Detective Control	A control activity designed to discover a fraudulent event or transaction after the initial processing has occurred. [Adapted from the COSO 2013 IC Framework]
Fraud Deterrence	The process of eliminating factors that may permit fraud to occur.
Fraud Preventive Control	A control activity designed to avoid a fraudulent event or transaction at the time of initial occurrence. [Adapted from the COSO 2013 IC Framework]
Fraud Response Plan	A policy aimed at ensuring that effective and timely action is taken in the event of fraud occurring. A Fraud Response Plan gives employees the details of the entire procedure for reporting any suspected fraud, defines the actions that the company needs to take and also defines authority levels, responsibilities for action, and reporting lines in the event of a suspected fraud or irregularity. [Source: Fraud.Net]
Fraud Risk Assessment	A dynamic and iterative process for identifying and assessing fraud risks to the achievement of objectives. Fraud risks to the achievement of objectives from across the entity are considered relative to established fraud risk tolerances. [Adapted from the COSO 2013 IC Framework]
Fraud Risk Governance	A Fraud Risk Management Program [that] should be in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding fraud risk. [Source: *Managing the Business Risk of Fraud: A Practical Guide*]
Fraud Risk Management Program	An organization's overall set of processes and procedures, including: • Fraud risk governance policies • Preventive and detective fraud control activities • Systems for monitoring the these policies and procedures • Fraud risk assessments • Fraud reporting mechanisms and fraud investigation protocals [Source: *Managing the Business Risk of Fraud: A Practical Guide*]
Fraud Risk Tolerance	The level of residual fraud risk that an organization is willing to accept that a fraudulent event or transaction will occur and not be detected in a timely manner.
Fraud Triangle	A model for explaining the factors that cause someone to commit occupational fraud. It consists of three components which, together, lead to fraudulent behavior: 1. Unshareable financial need (sometimes referred to as motive, incentive, or pressure) 2. Perceived opportunity 3. Rationalization [Source: Association of Certified Fraud Examiners]
Heat Map	A tool used to present the results of a risk assessment process visually and in a meaningful and concise way. A way of representing the resulting qualitative and quantitative evaluations of the probability of risk occurrence and the impact on the organization in the event that a particular risk is experienced. Organizations generally map risks on a heat map using a "residual risk" basis that considers the extent to which risks are mitigated or reduced by internal controls or other risk response strategies. [Source: CGMA Tools]
Inherent Risks	The risk to the achievement of objectives in the absence of any actions management might take to alter either the risk likelihood or impact. [Source: COSO 2013 IC Framework]
Insider Trading	Buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include "tipping" such information, securities trading by the person "tipped," and securities trading by those who misappropriate such information. [Source: Securities and Exchange Commission, "Fast Answers"]
Internal Control	A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance. [Source: COSO 2013 IC Framework]
Investigative Work Plan	A documented plan that should describe as many of the following components as deemed necessary: 1. Primary nature and complexity of the allegations (criminal, civil, and/or administrative); 2. Planned focus and objectives of the investigation; 3. Possible violation(s) of law, rule, or regulation and the corresponding elements of proof or standards; 4. Coordination with appropriate authorities, if warranted (another OIG, the Federal Bureau of Investigation, etc.); 5. Applicable judicial venue and coordination with prosecutors, when appropriate; 6. Steps necessary to meet investigative objectives; and 7. Resources necessary to meet investigative requirements. [Source: Council of the Inspectors General on Integrity and Efficiency, *Quality Standards for Investigations*]
Material/ Materiality	The omission or misstatement of an item in a financial report is material if, in light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item. [Source: FASB Statement of Financial Accounting Concepts No. 8, Chapter 3, as amended, QC11]
Management Override	Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition or compliance status. [Source: COSO 2013 IC Framework]
Market Capitalization	The total dollar market value of all of a company's outstanding shares. Market capitalization is calculated by multiplying a company's shares outstanding by the current market price of one share. The investment community uses this figure to determine a company's size, as opposed to sales or total asset figures. [Source: Investopedia]
Misappropriate/ Misappropriation	To embezzle or appropriate dishonestly for one's own use. [Source: AIS, Auditing Dictionary of Terms]

Glossary

Organizational Culture	Culture is the attitudes, behaviors, and understanding about risk, both positive and negative, that influence the decisions of management and personnel and reflect the mission, vision, and core values of the organization. The term organization is used to collectively describe the board of directors, management, and other personnel of an entity. [Source: Adapted from COSO 2017 ERM Framework]
Professional Skepticism	The ongoing questioning of whether the information and audit evidence obtained suggests that a material misstatement due to fraud may exist. It includes considering the reliability of the information to be used as audit evidence and the controls over its preparation and maintenance when relevant. Due to the characteristics of fraud, the auditor's professional skepticism is particularly important when considering the risks of material misstatement due to fraud. Although the auditor cannot be expected to disregard past experience of the honesty and integrity of the entity's management and those charged with governance, the auditor's professional skepticism is particularly important in considering the risks of material misstatement due to fraud because there may have been changes in circumstances. [Source: Paragraphs .A9 and .A10, AU-C sec. 240, *Consideration of Fraud in a Financial Statement Audit*]
Related-Party Transactions	Depending on the context, "related parties" can be a very broad concept. See, for example, the definition in FASB Accounting Standards Codification, Master Glossary: a. Affiliates of the entity; b. Entities for which investments in their equity securities would be required, absent the election of the fair value option under the Fair Value Option Subsection of Section 825–10–15, to be accounted for by the equity method by the investing entity; c. Trusts for the benefit of employees, such as pension and profit-sharing trusts that are managed by or under the trusteeship of management; d. Principal owners of the entity and members of their immediate families; e. Management of the entity and members of their immediate families; f. Other parties with which the entity may deal if one party controls or can significantly influence the management or operating policies of the other to an extent that one of the transacting parties might be prevented from fully pursuing its own separate interests; and/or g. Other parties that can significantly influence the management or operating policies of the transacting parties or that have an ownership interest in one of the transacting parties and can significantly influence the other to an extent that one or more of the transacting parties might be prevented from fully pursuing its own separate interests.
Reputation Risk	The potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions. [Source: Federal Reserve System, Supervisory Policy and Guidance Topics]
Residual Fraud Risk	The initial assessment of fraud risk should consider the inherent risk of particular frauds occurring in the absence of internal controls. After all relevant fraud risks have been identified, internal controls are mapped to the identified risks. Fraud risks that remain unaddressed by appropriate controls comprise the population of residual fraud risks. [Source: *Managing the Business Risk of Fraud: A Practical Guide*]
Risk Appetite	Is the types and amount of risk, on a broad level, an organization is willing to accept in pursuit of value. [Source: COSO 2017 ERM Framework]
Risk Assessment	Risk is defined as the possibility that an event will occur and adversely affect the achievement of objectives. Risk assessment involves a dynamic and iterative process for identifying and assessing risks to the achievement of objectives. Risks to the achievement of these objectives from across the entity are considered relative to established risk tolerances. Thus, risk assessment forms the basis for determining how risks will be managed. [Source: COSO 2013 IC Framework]
Risk Tolerance	The acceptable variation relative to performance to the achievement of objectives. [Source: COSO 2013 IC Framework]
Segregation of Duties	The separation of the authority, custody, and accounting of an operation. [Source: Government Accountability Office (GAO), Standards for Internal Control in the Federal Government, see page 78]
Stakeholders	Parties that are affected by the entity, such as shareholders, the communities in which an entity operates, employees, customers, and suppliers. [Source: COSO 2013 IC Framework]
Statistical Analysis/ Predictive Modeling	*Statistical analysis* is a component of data analytics. In the context of business intelligence, statistical analysis involves collecting and scrutinizing every data sample in a set of items from which samples can be drawn. [Source: WhatIs.com] *Predictive modeling* is a process used in predictive analytics to create a statistical model of future behavior. Predictive analytics is the area of data mining concerned with forecasting probabilities and trends. In predictive modeling, data is collected for the relevant predictors, a statistical model is formulated, predictions are made, and the model is validated or revised as additional data becomes available. [Source: TechTarget SearchDataManagement]
Tolerance	The boundaries of acceptable variation in performance related to achieving business objectives. [Source: COSO 2017 ERM Framework]
Top-Side Entries/ Adjustments	Widely considered among the riskiest types of journal entries in accounting, topside entries occur when a corporate entity makes financial entries on its subsidiaries journals. While top-side entries can be legitimate and coincide with generally accepted auditing standards, they can also be used to make fraudulent transactions appear legitimate. [Source: Miranda Morley, What Is a Topside Entry in Accounting?]
Trade Secrets	Any practice or process of a company that is generally not known outside of the company. Information considered a trade secret gives the company an economic advantage over its competitors, and is often associated with internal research and development. In order to be legally considered a trade secret in the United States, a company must take a reasonable effort in concealing the information from the public, the secret must intrinsically have economic value and the trade secret must contain information. [Source: Investopedia]
Transaction-Level Control Procedures	A control activity that directly supports the actions to mitigate transaction processing risks in an organization's business processes. Transaction controls can be manual or automated and likely cover the information-processing objectives of completeness, accuracy, and validity. [Source: COSO 2013 IC Framework]
Whistleblower	Anyone who has and reports insider knowledge of illegal activities occurring in an organization. Whistleblowers can be employees, suppliers, contractors, clients, or any individual who somehow becomes aware of illegal activities taking place in a business either through witnessing the behavior or being told about it. Whistleblowers are protected from retaliation under various programs created by the Occupational Safety and Health Administration (OSHA) and the Securities and Exchange Commission (SEC). [Source: Investopedia]
Whistleblower System	Reporting mechanisms that facilitate reporting of allegations regarding fraudulent, illegal, or unethical conduct. Such mechanisms can include telephone hotlines, dedicated email addresses, web-based or online reporting, or ombudsmen. [For more information on whistleblower systems, see ACFE's *Reports to the Nations*]

APPENDIX B

Fraud Risk Management Roles and Responsibilities

This appendix is adapted from Appendix B (*Roles and Responsibilities*) of the 2013 COSO *Internal Control — Integrated Framework*,[14] with COSO's permission.

Introduction

Fraud risk management is effected by personnel internal to the organization, including the board of directors, the audit committee if applicable, senior management, internal audit, business-enabling functions, risk and control personnel, legal and compliance personnel, specialists, as well as other parties interacting with the organization. Everyone associated with the organization, all employees, customers, vendors, and stakeholders observe day-to-day operations and activities, and are encouraged to report any suspicious transactions, relationships, or behaviors. Collectively, all contribute to an effective fraud risk management system.

An organization may view fraud risk management through three lines of defense:

- Management and other personnel on the front line provide the first line of defense against fraud as they are responsible for maintaining effective vigilance and carrying out fraud control activities; they are charged with carrying out the Fraud Risk Management Program through day-to-day operations.
- Management and other personnel on the front line also provide second line roles through their expertise, support, monitoring, and challenge on fraud risk related matters.
- Internal auditors provide third line roles as they assess and report on internal control, fraud prevention and detection activities, and recommend corrective actions or enhancements for management to consider and implement.

Responsible Parties

Every individual within an organization has a role in effecting fraud risk management. Roles vary in responsibility and level of involvement, as discussed below.

Board of Directors and Audit Committee

The board is responsible for overseeing the Fraud Risk Management Program as well as the system of internal control. With the power to engage or terminate the chief executive officer (CEO), the board has a key role in defining expectations about integrity and ethical values, transparency, and accountability for the implementation and operation of the Fraud Risk Management Program. Board members are objective, capable, and inquisitive. They have a working knowledge of the organization's activities and environment, and they commit the time necessary to fulfill their governance responsibilities. They utilize resources as needed to investigate any issues, and they have an open and unrestricted communications channel with all organization personnel, the internal auditors, external auditors, external reviewers, and legal counsel.

Regulatory and professional standard-setting bodies often require the use of audit committees. The role and scope of authority of an audit committee can vary depending on the organization's regulatory jurisdiction, industry norm, or other variables. For example, in certain jurisdictions the audit committee is charged with overseeing the external auditor's work and directly responsible for the auditor's appointment and compensation. This is sometimes also inclusive of a broader risk mandate and identified as the audit and risk committee to clearly describe the risk oversight.

Management is responsible for the reliability of the financial statements, but an effective audit committee plays a critical oversight role. The board of directors, often through its audit committee, has the authority and responsibility to question senior management regarding how it is carrying out its internal and external reporting responsibilities and to verify that the organization takes timely corrective actions, as necessary.

As a result of its independence, the audit committee, along with a strong internal audit function, is often best positioned to identify and promptly act in situations where senior management overrides controls or deviates from expected standards of conduct. The audit committee interacts with the external auditors, meeting regularly to discuss the scope of planned audit procedures and results of audit procedures. Meetings with the external auditors include executive sessions without management present to provide a forum for further dialogue between the independent auditors and audit committees.

An audit committee of the board of directors that is committed to a proactive approach to fraud risk management plays an active role in the fraud risk assessment process and uses the internal audit department to monitor fraud risks.[15]

The audit committee is expected to be aware of the fraud risks common in the industries in which the organization operates. The audit committee develops its own views as to what represent significant fraud risks to the organization. In developing those views, the audit committee considers the professional guidance that the independent auditors are required to follow.

The audit committee seeks the advice of counsel whenever it is dealing with allegations of fraud. Because fraud allegations are serious, there may be a legal duty to investigate or report them, which falls under the purview of the legal department or outside counsel. (See Chapter 4, which encompasses the various investigative channels and best practices available to investigate fraudulent activities.)

For publicly traded companies (and some other organizations) the audit committee is composed of independent board members, with at least one member who is a financial expert, preferably with an accounting background.[16] The committee meets frequently enough, for long enough periods, and with sufficient preparation, to adequately assess and respond to the risk of fraud, especially management fraud, because such fraud typically involves override of the organization's internal control.

At each meeting, the audit committee meets separately with its external audit firm and the chief internal audit executive, if applicable, to provide a forum for open dialogue, with a significant focus on detecting fraud that has a direct impact on the organization's finances. In addition, since reputation risk resulting from fraudulent behavior often has a severe impact on stakeholder value, the audit committee provides specific consideration and oversight of such exposure when assessing the work of management, internal auditors, and external auditors.

While board composition requirements vary, independent directors are important as they can provide an objective perspective. For example, the UK, German, and other corporate governance codes, and the New York Stock Exchange (NYSE) and NASDAQ listing requirements define the number of and criteria for audit committee members to be independent from management and financially literate (e.g., at least one member with accounting or financial management expertise). This independence is vital to sound fraud risk management.

External independent auditors have a responsibility to plan and perform the audit of the organization's financial statements taken as a whole to obtain reasonable assurance about whether the financial statements are free of material misstatement due to fraud.[17] External independent auditors, as part of the audit, among other things:

- Consider events or conditions that indicate incentives/pressures to perpetrate fraud, opportunities to carry out the fraud, and attitudes/rationalizations to justify a fraudulent action. (Chapter 2 discusses the Fraud Triangle in greater detail.)
- Brainstorm among the audit team members about how and where they believe the organization's financial statements might be susceptible to material misstatement due to fraud.
- Inquire of management and others within the organization about the risks of fraud.
- Perform analytical procedures to identify unusual transactions or events and amounts, ratios, and trends that might indicate matters that have financial statement implications.

Additionally, whenever the independent auditor has determined that there is evidence that fraud may exist or has occurred, the auditor's professional standards provide that the matter should be brought to the attention of an appropriate level of management and, in certain circumstances, to those charged with governance.[18] Further, management evaluates the possible risk associated with the evidence of fraud.[19]

Senior Management

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. An organization's culture plays an important role in deterring, preventing, and detecting fraud.

It is important that senior management creates a culture through its words and actions so that it is clear that fraud is not tolerated, that any such behavior is dealt with swiftly and decisively, and that whistleblowers will not suffer retribution. Fairness and consistency in dealing with fraud are important, particularly with regard to how both high-level and low-level personnel are treated.

The CEO is accountable to the board of directors and is responsible for designing, implementing, and conducting an effective Fraud Risk Management Program. In privately owned, not-for-profit, or other entities, the equivalent role may have a different title but generally covers the same

[14] COSO, *Internal Control — Integrated Framework* (May 2013).

[15] In governmental organizations, there may not be an audit committee, per se. There may be an audit advisory committee, legislative oversight organization, or some other body that performs a similar function.

[16] See 17 CFR PARTS 228, 229, 240, 249, and 274 and SEC Rule RIN 3235-AI75. [See sec.gov/rules/final/33-8220.htm#back]. For other organizations, this audit committee composition is not required, but is recommended.

[17] See paragraph .06 of AU-C sec. 200, Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards, [See aicpa.org/research/standards/auditattest/downloadabledocuments/au-c-00200.pdf.]

[18] See paragraph .39 of AU-C sec. 240, Consideration of Fraud in a Financial Statement Audit. [See aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-C-00240.pdf.]

[19] The SEC's interpretative guidance for management with respect to internal controls (SEC Interpretive Release 33-8810, p. 14 [See sec.gov/rules/interp/2007/33-8810.pdf]) states: Management's evaluation of the risk of misstatement should include consideration of the vulnerability of the entity to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets, and corruption), and whether any such exposure could result in a material misstatement of the financial statements. Management should recognize that the risk of material misstatement due to fraud ordinarily exists in any organization, regardless of size or type, and it may vary by specific location of segment and by individual financial reporting element.

responsibilities, as described below. More than any other individual, the CEO sets the tone at the top that affects the control environment and all other components of internal control and fraud risk management.

The CEO's responsibilities relating to fraud risk management include:

- Providing leadership and direction to senior management and shaping the organization's values, standards, expectations of competence, integrity, organizational structure, and accountability that form the foundation of the organization's fraud risk management system
- Maintaining oversight and control over the fraud risks facing the organization
- Guiding the development and performance of fraud control activities at the entity level and delegating to various levels of management the design, implementation, conduct, and assessment of fraud control activities at different levels of the entity
- Communicating expectations regarding the organization's fraud risk tolerance (e.g., integrity, competence) and potential fraud information reporting expectations (e.g., the hotline reporting system the organization will use)
- Evaluating fraud risk assessments and the impact on the ongoing and long-term effectiveness of the Fraud Risk Management Program

Senior management comprises not only the CEO but also other senior executives leading the key operating units and business-enabling functions. Examples include:

- Chief administrative office
- Chief audit executive
- Chief compliance officer
- Chief financial officer
- Chief information officer
- Chief legal officer
- Chief operating officer
- Chief risk officer
- Other senior leadership roles, depending on the nature of the business

These senior management roles support the CEO with respect to fraud risk management by reinforcing the CEO's responsibilities and leadership and ensuring that these values and requirements are carried out in their specific areas of responsibility.

In meeting its responsibilities, senior management reports to the board regularly on the effectiveness of the Fraud Risk Management Program and recommends any remedial steps that are needed.

Internal Audit

Internal audit uses a risk-based approach in its planning and prioritization, linked to the goals of the organization. Within that risk-based approach, is a focus on fraud risk. The following are specific roles and responsibilities related to fraud risk.

Internal audit[20] ensures that the audit committee is made aware of instances of fraud, the results of investigations into fraud, corrective actions, and monitoring plans. In addition, internal audit considers the use of data analytics as a means of performing proactive monitoring of high-risk areas. (See Appendix D for additional discussion of data analytics and fraud.)

Internal audit also assesses the ongoing governance framework by verifying that all employees have attended required ethics training and completed any required forms, such as conflict of interest and code of conduct forms. In addition, internal audit also examines trends related to violations and fraud investigations.

Internal audit also provides reasonable assurance that fraud prevention and detection controls are sufficient for identified fraud risks and ensures that the controls are functioning as designed. Although the independent auditors primarily focus on fraudulent financial reporting, an effective internal audit department focuses on potential fraud for all of its executed audits, which typically span a much larger segment of the organization than the independent auditors address. In many instances, the internal audit group leads various fraud working groups within an organization and assists in identifying potential fraud scenarios. (See Chapter 2 for more information about the tools and processes associated with executing an effective fraud risk assessment while establishing a continual focus on fraud detection and prevention throughout an organization.)

Some fraud risks are straightforward and consistent in nature, such as weak segregation of duties in a warehousing operation or in the purchasing function. Other risks, such as cybersecurity, have a much more volatile and changing risk profile. Given the dynamic nature of cybersecurity and the potential effect that it may have on the organization, many boards of directors approach cyber risk from an enterprise-wide standpoint. This approach includes understanding the risks of cyber fraud from a legal standpoint. In areas such as cyber fraud, the board may require access to outside expertise to enable well-informed interactive discussions with senior leadership.

Business-Enabling Functions

Various organizational functions or operating units support the organization through specialized skills, such as enterprise risk management, internal control oversight, finance, product/service quality management, technology, compliance, legal, human resources, and others. They provide guidance, assess fraud risk, and assess fraud risk management activities related to their areas of expertise, and it is incumbent on them to share and evaluate issues and trends that transcend organizational units or functions. They keep the organization informed of relevant requirements that might affect fraud risk as they evolve over time.

While all fraud control activities function to serve a purpose, their efforts are coordinated and integrated as appropriate. For example, a company's new customer acceptance process may be reviewed by the compliance function from a regulatory perspective, by the risk management function from a concentration risk perspective, and by the internal audit function to assess the design and effectiveness of controls. Disruptions to the business process are minimized when the timing and approach to reviews and management of issues are coordinated to the extent possible. Integration of efforts helps create a common language and platform for evaluating and addressing fraud risks.

Risk and Control Personnel

Risk and control functions are key parts of fraud risk management. Depending on the size and complexity of the organization, dedicated risk and control personnel may support functional management to manage different fraud risk types (e.g., operational, financial, quantitative, qualitative) by providing specialized skills and guidance to front-line management and other personnel and evaluating fraud control activities. These functions can be part of an organization's centralized or corporate organization, or they can be set up with "dotted line" reporting to functional heads. Risk and control functions are central to the way management maintains control over business activities.

Responsibilities of risk and control personnel include identifying known and emerging fraud risks, helping management develop processes to manage such relevant risks, communicating and providing education on these processes across the organization, and evaluating and reporting on the effectiveness of such processes. The chief risk/control officer is responsible for reporting to senior management and the board on significant fraud risks to the business and whether these risks are managed within the organization's established fraud risk tolerance levels, with adequate prevention and detection controls in place.

Legal and Compliance Personnel

Counsel from legal professionals is key to defining effective fraud control activities for compliance with regulations and mitigating litigation risks. In large and complex organizations, specialized compliance professionals can be helpful in defining and assessing fraud control activities for adherence to the organization's Fraud Risk Management Program. The chief legal compliance officer is responsible for ensuring that legal, regulatory, and other requirements are understood and communicated to those responsible for effecting compliance.

A close working relationship between business management and legal and compliance personnel provides a strong basis for designing, implementing, and conducting fraud risk management control activities to manage adverse outcomes, such as regulatory sanctions, legal liability, and failure to adhere to internal compliance policies and procedures. At smaller organizations, legal and compliance roles may be shared by the same professional, or one of these roles can be outsourced with close oversight by management.

Specialists

In addition to the audit committee, internal audit, and management, the organization also may include professionals with specific domain expertise, e.g., legal, compliance, investigations, emerging markets, human resources, geographic/cultural, and technology.

Organizations integrating data analytics into their fraud risk programs also include personnel with the appropriate technical skills. Organization size and complexity are factors in determining the extent to which data analytics are integrated into a Fraud Risk Management Program.

Organizations consider how to address three distinct skill sets when incorporating data analytics into the fraud risk program:

- **Information technology skills —** Familiarity with the various information technology systems within the organization and the ability to assist with acquiring and assessing the necessary internal or external data sources for analysis
- **Business domain knowledge skill —** Familiarity with fraud risk areas within the business domain under analysis and the ability to design appropriate fraud risk questions and to appropriately challenge and interpret the analytics results
- **Data science skills —** Ability to extract knowledge from the data, including mathematical and business intelligence techniques, such as statistics, pattern recognition, data-base design, data visualization, and query design

Typically, these skills are not maintained by a single individual, so it is important for the fraud risk working group to take inventory of the available skills in-house and to then seek additional data analytics assistance as required.

All Employees

Understanding the effects of fraud and the importance of preventing fraud is the responsibility of each person in the organization. It encompasses:

- Understanding the organization's ethical culture and the organization's overall commitment to that culture
- Understanding one's individual role within the fraud risk management framework
- Understanding the importance of the Fraud Risk Management Program and how fraud can negatively impact the organization on multiple fronts
- Reading, understanding, and upholding the fraud risk management policy as well as other operational policies, such as procurement and whistleblower policies
- As required, participating in the process of improving the Fraud Risk Management Program by designing and implementing control activities as well as participating in monitoring activities
- Understanding fraud indicators and risk factors as they pertain to one's responsibilities and understanding the necessity to report indicators of potential fraud through various channels that might be dependent upon the source of the information
- Understanding how and to whom to report possible instances of fraud
- Having a clear understanding that the organization has the right to institute civil or criminal action against anyone who commits fraud

[20] Not all organizations have an internal audit group or function, and some organizations (such as governmental organizations) have oversight bodies (e.g., inspectors general or legislative auditors) that perform a similar function. [See Appendix G, Managing the Risk of Fraud, Waste, and Abuse in the Government Environment.]

Other Parties Interacting with the Organization
Customers, vendors, and others transacting business with the organization are an important source of information used in managing fraud risk. For example:

- A customer can inform a company about undelivered goods, inferior product quality, or the failure to otherwise meet the customer's expectations; and these might be indicators of possible fraudulent activity.
- A vendor can provide statements or information regarding unusual or anomalous transactions or actions by the organization's employees.
- A potential supplier can notify senior management of an employee's request for a kickback.

Such information sharing between management and external parties can be important to the organization in achieving its fraud risk management objectives. The organization has mechanisms in place with which to receive such information and to take appropriate action on a timely basis — that is, it not only addresses the particular situation reported, but also investigates the underlying source of an issue and fixes it.

In addition to customers and vendors, other parties, such as creditors, can provide insight on the achievement of an organization's fraud risk management objectives. A bank, for example, may request reports on an organization's compliance with certain debt covenants and recommend performance indicators or other desired targets or controls.

APPENDIX C

Fraud Risk Management Considerations for Smaller Entities

This appendix is adapted from Appendix C (*Considerations for Smaller Entities*) of the COSO 2013 IC Framework, with COSO's permission.

Characteristics of Smaller Entities

Many different perceptions exist as to what constitutes a "smaller" entity. Some think of a local, family-owned hardware store or corner bakery as a typical small business. Others may think of a not-for-profit entity that generates several million dollars in annual donations. Others think of a small governmental organization, such as a small town or county or a small government agency. Others may consider a small entity in the context of a company that has been public for many years that manufactures an innovative product and now generates annual revenue of several hundred million dollars, with hopes that future growth will catapult it to the Fortune 500 category. Depending on one's perspective, any or all of these may be considered "smaller" entities.

COSO does not provide a definition of a smaller entity in terms of revenue, capitalization, or other factors; that is the role of regulators or other parties. Instead, the term "smaller" rather than "small" suggests there is a wide range of entities to which these considerations apply. The focus here is on smaller entities that have many of the following characteristics:

- Fewer lines of business and fewer products within lines
- Concentration of marketing focus by channel or geography
- Leadership by management with significant ownership interest or rights
- Fewer levels of management with wider spans of control
- Less complex transaction processing systems
- Fewer personnel, many having a wider range of duties
- Limited ability to maintain deep resources in line as well as support staff positions such as legal, human resources, accounting, and internal auditing

The last bulleted item, limited ability to maintain deep resources, is a frequent cause of smaller entities being lower on the economies-of-scale curve. Often, but not always, smaller entities have a higher per unit cost of producing a product or providing a service. On the other hand, many smaller entities achieve competitive advantage in cost savings through innovation, lower overhead (by retaining fewer people and substituting variable for fixed costs via a part-time workforce or variable compensation plans), and a narrower focus in terms of product, location, and complexity.

Economies of scale is often a factor affecting support functions, including those that directly support internal control and fraud risk management. For example, establishing an internal audit function within a hundred-million-dollar entity likely would require a larger percentage of economic resources than would be the case for a multi-billion-dollar entity. Certainly, the smaller entity's internal audit function would be smaller and might rely on co-sourcing or outsourcing to provide needed skills, whereas the larger entity's function might have a broad range of experienced personnel in-house. But in all likelihood, the relative cost for the smaller entity would be higher than for the larger one.

None of the above characteristics by themselves are definitive. Certainly, size, by whatever measure — assets, revenue, spending, personnel, or other — affects and is affected by these characteristics and shapes thinking about what constitutes "smaller."

Meeting Challenges in Attaining Cost-effective Fraud Risk Management

The characteristics of smaller entities tend to provide challenges for cost-effective fraud risk management. Often managers of smaller entities view internal control and fraud risk management as administrative burdens to be added to existing business processes, rather than recognizing the business need for and benefit of effective internal control and fraud risk management that is integrated within these processes.

Another major challenge to effective fraud risk management in smaller organizations is a perception that, "fraud cannot happen here, it only happens to other organizations." Similarly, smaller organizations might tend to think that they hire only honest people and, therefore, that they trust their employees.

Among other challenges to smaller entities are:

- Obtaining sufficient resources to achieve adequate segregation of duties
- Balancing management's ability to dominate activities, with significant opportunities for improper management override of processes in order to appear that business performance goals have been met
- Recruiting individuals with requisite expertise to serve effectively on the board of directors and committees
- Recruiting and retaining personnel with sufficient experience and skill in operations, reporting, compliance, and other disciplines
- Taking critical management attention from running the business in order to provide sufficient focus on internal control and fraud risk management
- Controlling information technology and maintaining appropriate general and **application controls** over computer information systems with limited technical resources
- Limited technical resources and expertise in data analytics

Despite resource constraints, smaller entities usually can meet these challenges and succeed in implementing effective fraud risk management in a reasonably cost-effective manner.

In terms of cost-benefit considerations, one thing is clear: the costs and impact of being victimized by fraud can be and often are devastating. While this is true for organizations of any size, ACFE research has shown that smaller organizations tend to be victims of fraud more than larger organizations, and the impact to smaller organizations is much greater, proportionately, than the impact to larger organizations. Any organization that has been victimized by fraud will affirm that, in retrospect, it should have implemented a more rigorous fraud risk management process.

Segregation of Duties
Many smaller entities have limited numbers of employees performing various functions, which sometimes results in inadequate segregation of duties. There are, however, actions that management can take to compensate for this circumstance. Following are some types of fraud control activities that can be implemented:

- **Control access to accounting records and check stock —** Do not allow employees who maintain accounting records to have direct access to check stock.
- **Control access to bank statements —** Direct financial institutions to send statements to individuals who do not have access to the checkbook or accounting records.
- **Control bank account reconciliations —** Have bank reconciliations performed by individuals who do not have access to the checkbook or accounting records.
- **Review reports of detailed transactions —** Have managers review on a regular and timely basis system reports of the detailed transactions.
- **Review selected transactions —** Have managers select transactions for review of supporting documents.
- **Periodically observe assets —** Have managers periodically conduct counts of physical inventory, equipment, and other assets and compare them with the accounting records.
- **Perform reconciliations —** Have managers, from time to time, review reconciliations of account balances, such as cash, accounts payable, and accounts receivable, or perform them independently.

Segregation of duties is not an end in itself. Rather, it is a means of mitigating a risk inherent in processing transactions. When developing or assessing fraud control activities that address risks in an entity with limited ability to segregate duties, management considers whether other controls satisfactorily address these risks and are applied conscientiously enough to reduce fraud risk.

Management Override
Many smaller entities are dominated by the founder or a leader who exercises a great deal of discretion and provides personal direction to other personnel. This positioning may be key to enabling the entity to meet its growth and other objectives and can also contribute significantly to effective internal control and fraud risk management. With this leader's in-depth knowledge of different facets of the entity — its operations, processes, policies and procedures, contractual commitments, and business risks — he or she is positioned to know what to expect in reports generated by the system and to follow up as needed. Such concentration of knowledge and authority, however, comes with a downside: the leader typically is able to override controls.

There are a few basic but important things that can help to mitigate the risk of management override:

- Maintain a corporate culture in which integrity and ethical values are held in high esteem, embedded throughout the organization, and practiced on an everyday basis. This can be supported and reinforced by recruiting, compensating, and promoting individuals so that these values are appropriately reflected in behavior.
- Implement a whistle blower system that allows personnel to feel comfortable reporting any improprieties, regardless of the level at which they may be committed. Importantly, they may be able to maintain anonymity and confidence that reported matters will be investigated thoroughly and acted upon appropriately and without reprisals. It is important that, where circumstances warrant, matters can be reported directly to the board or audit committee.
- Position an effective internal audit function to detect instances of wrongdoing and breakdowns at the entity and subunit levels. Ready access to relevant information and ability to communicate directly with senior management and the board or audit committee are key factors.
- Attract and retain qualified board members who take their responsibilities seriously to perform the critical role of preventing or detecting instances of management override. Such practices mitigate the risk of impropriety and promote accountability of leadership, while gaining the unique advantages of cost-effective internal control and fraud risk management in a smaller entity environment.

Board of Directors

The discussion above highlights the need for a board of directors with requisite expertise to perform its oversight responsibilities well. With appropriate knowledge, attention, and communication, the board is positioned to provide an effective means of offsetting the effects of improper management override. In smaller entities, the board of directors typically has in-depth knowledge of what usually are relatively straightforward business operations, and it communicates more closely with a broader range of personnel.

Many smaller entities, however, find it very difficult to attract independent directors with the desired skills and experience. Typical challenges to finding suitable directors include potential board members' inadequate knowledge of the entity and its people, the entity's limited ability to provide compensation commensurate with board responsibilities, a sense that the chief executive might be unaccustomed or unwilling to appropriately share governance responsibilities, or concerns about potential personal liability.

Some entities address such concerns about desired board candidates and expand their search of valued or required expertise to include, for example, financial and accounting expertise. In this way, they can shape the board to not only appropriately monitor senior management, but also to provide value-added advice.

Fraud Reporting (Whistleblower) Systems

Until recently, maintaining and operating a whistleblower hotline was a relatively expensive undertaking that often went well beyond the means of most smaller entities. Third-party web-based systems are now available to smaller entities at a modest cost. Such systems have the advantages of not only low cost, but also greater assurance of reporter anonymity, the ability to ask follow-up questions of reporters without fear of exposing their identities, and tested intake questionnaires. Small entities will exercise caution, however, before engaging such a service. The service's information security controls must be carefully reviewed to ensure that sensitive information is fully protected.

The strong deterrent value of having a whistleblower system in place almost certainly outweighs the cost of using a third-party service.

Data Analytics

As discussed throughout this Guide, data analytics is one of the strongest and most effective means of managing fraud risk. However, smaller entities may not have the technical resources and personnel necessary to select, develop, and deploy data analysis applications in a controlled or sustainable manner. Thus, these entities consider alternatives to meeting their needs related to fraud risk management.

It is important for small entities to understand the current data analytic software capabilities in the market as many business and accounting software packages include a variety of standard reports that can be run and reviewed regularly. A helpful resource for any size organization is the AICPA's "Understanding the forensic technology landscape: A reference guide for practitioners" which outlines various commercial and open source technologies available and their practical use-case applications.

Simple but effective tests, for example, can be run using Microsoft (MS) Excel. Such tests include examining the top and bottom records by sorting the file (by amount, by date, by employee number, by policy number, etc.) to identify unusual entries. Data can be extracted by period or location and MS Excel can produce a trend analysis to identify anomalies. Filters can help identify unusual entries. Data can be sorted by sales person or cash register, and filters can be used to identify returns, overrides, etc. Many insightful analytics can also be accomplished via MS Excel's use of pivot tables.

Smaller entities can also retain consultants or ask external auditors to run specific tests that focus on areas of high-risk or have specialized reports developed to monitor these areas. In addition, commercially developed data analysis packages and data visualization tools can be very effective in carrying out an array of data analysis tests. These programs tend to be menu-driven and user friendly, enabling personnel with minimal training and experience to carry out tests as part of the entity's fraud control activities.

Monitoring Activities

Monitoring activities routinely performed by managers running a business can provide information on the presence and functioning of the other fraud risk management principles. Management of many smaller entities regularly perform such activities, but have not always taken sufficient credit for their contribution to the effectiveness of internal control and fraud risk management. These activities, usually performed manually and sometimes supported by computer software, are fully considered in designing, implementing, and carrying out fraud risk management processes and the effectiveness of the Fraud Risk Management Program.

The Advantages of Smaller Entities in Attaining Cost-effective Fraud Risk Management

Many of the challenges to smaller entities described above are mitigated to a great degree by the fact that smaller entities are usually less complex in structure and operations. This makes the fraud risk assessment easier to perform. Where larger, complex entities might need to assemble several risk assessment teams to address all areas of operations, the smaller entity can often carry out the risk assessment with a smaller team of individuals with knowledge of all areas of operations.

In a large, complex entity, the chances are greater that a significant fraud risk might be overlooked. In a smaller entity, greater assurance can be obtained that all significant fraud risks are identified and mitigated.

APPENDIX D

Data Analytics

Data analytics continue to evolve and are becoming increasingly more powerful and important tools in efforts to prevent, detect, and deter fraud. This Guide contains three appendices on data analytics to explore key aspects of their use.

- **Appendix D-1** explains how to build a sustainable data analytics capability, develop a data analytics plan, attract and develop a team of skilled professionals, acquire the right technological solutions, and implement processes and procedures. A comprehensive and sustainable data analytics capability supports both fraud risk management and operational areas, such as internal audit and investigations.
- **Appendix D-2** provides both guidance and practical examples of the application of data analytics techniques and approaches as part of a fraud risk assessment.
- **Appendix D-3** explains how data analytics techniques can enhance fraud control activities to mitigate residual risks that were identified during the fraud risk assessment.

APPENDIX D.1

Data Analysis — Building a Sustainable Data Analytics Capability

This appendix explains how to build a sustainable data analytics capability, including the following key elements:

- Developing a data analytics plan
- Attracting and developing a team of data analytics professionals
- Acquiring the right technological solutions
- Developing and maintaining data analytics processes and procedures

Surveys by the ACFE and professional services firms over the past 10 to 15 years have consistently rated data extraction, data analysis, and analytical software as critical tools for effective internal audit functions. A comprehensive and sustainable data analytics capability supports both fraud risk management and operational areas, such as internal audit and investigations.

Developing a Data Analytics Plan

Data analytics support all aspects of fraud risk governance, risk assessment, control activities, investigation and communication, and monitoring. The starting point is a sound plan to develop or enhance data analytics capabilities.

Ideally the plan includes the following elements and characteristics:

- Articulates a commitment to the integration of data analytics
- Considers the need for staffing at the appropriate level, skills, knowledge, and number

- Roles and responsibilities are assigned, with objectives, milestones, and reporting requirements
- Technologies are specified, including software and hardware
- Links directly to the fraud risk assessment
- Has appropriate sponsorship and oversight from management and those charged with governance
- Articulates Objectives, Goals, Strategies, and Measures (OGSM) for the use of analytics

A sample OGSM statement follows:

Sample OGSM Statement

Objectives
- Data analytics and AI capability will be used to add significant value to the fraud risk management process.
- Data analytics will be used to transform the efficiency, effectiveness, and value-add of the fraud risk management process.
- Data analytics is a key driver of an integrated approach to audit, fraud risk identification and assessment, control testing, and potential fraud investigation.

Goals
Reduce and mitigate the organization's exposure to fraud risk by leveraging traditional and data analytics tools to prevent, promptly detect, and respond to identified fraud risks as part of the Fraud Risk Management Program.

Strategies
- Identify guidance and resources to support employees in obtaining and analyzing data.
- Identify or develop training that will enable staff to leverage analytics in their roles.
- Identify key data sets, analytic tools, techniques, and approaches, including visualization and advanced analytics, to support the organization's Fraud Risk Management Program.

Measures
- X% of fraud risk identification and assessment planning processes will include quantitative analytics.
- Data analytics will be used on X% of fraud risk assessments and Z% of audits and investigations within a Y-month timeframe.
- Reduction in the cycle time of X% for audits and investigations using data analytics.
- Data analytics will result in an X% increase in positive feedback about value-added by audit and investigative personnel.
- X fraud risk assessments will include automated repeatable analysis routines by Y date.
- X% reduction in hours spent on manual controls testing procedures.

Attracting and Developing a Team of Data Analytics Professionals
A variety of roles and skills are needed to support a data analytics capability. These roles often evolve as data analytics capabilities become more mature within an organization. Team leaders need a good understanding of the different roles and how to organize them to the best effect.

The success of an analytics program depends heavily upon the people, knowledge, and skill sets available. In addition to those charged with governance, such as the audit committee of the board, internal audit, and other functions involved in managing fraud risk, the organization may also look to professionals with specific domain expertise, such as legal, enterprise risk management, regulatory compliance, security, emerging markets, human resources, those with geographic or cultural knowledge, and information technology experts. Few of these skills will be provided by junior level programming resources. These skills rarely exist within one individual, and they might not already exist collectively in the organization. Often, needed skills are assembled from a mix of internal and external resources. Planning includes establishing an inventory of the required knowledge and skills and determining how to best meet those needs through training and improving the experience of human resources.

Planning is based on an understanding of the business processes, the data supporting them, the investigation processes and requirements, and the application of relevant professional and legal standards.

Organization size and complexity are factors in determining the extent to which data analytics are integrated into a Fraud Risk Management Program. A good place to start developing the fraud risk management analytics capability is within the internal audit function. Internal auditors frequently leverage analytics and their knowledge of the underlying systems, data, and analytics prepares them to support audits, risk assessments, or investigations. Internal audit personnel already know the business processes, have the audit and investigative skills, and perhaps have some analytical capabilities. However, they need to be supported by training and software and given sufficient time to develop the skills and implement the functionality. It is also best practice that internal audit teams meet with compliance and legal personnel to address certain regulatory and compliance risks, which also includes the need for compliance professionals to conduct proactive monitoring of third-party risk activities — such as data privacy, anti-corruption, anti-money laundering, among other regulatory risks. Once the organization has committed to a data analytics function, its use will become the norm. A decision to omit data analytics in any situation should be an informed decision, supported by a costs and benefits analysis.

Acquiring the Right Technological Solutions
A common question for organizations just starting out on data analytics is which software tools to use. The answer depends on the organization's requirements and short- and long-term plans for analytics. Existing capabilities, such as standard reports and Excel, are good starting points. There is an increasing number of analytic software options that can increase capabilities.

Fraud risk management teams work closely with the information technology (IT) function to ensure the implementation of analytics is successful. Most of the interaction with IT typically occurs in the context of software selection and data access and extraction. In part, the extent of interaction depends upon the availability within the fraud risk management function of technical expertise and data access and extraction software. Software considerations include:

- **Data Access** — the ability to connect to internal and external systems
- **Data Extraction** — the ability to pull required data from internal and external sources in an efficient and secure manner
- **Data Transformation or Cleansing** — the process of preparing data extracts into data that is formatted, validated, and available for analysis
- **Data Analysis** — the analysis of data from statistical, business process, and IT controls, and examining outliers, relationships, and use of AI
- **Data Mining** — the examination of internal and external data sources, both structured and unstructured
- **Visualization** — the presentation of results in a visual format for consumption by senior management
- **Dashboarding** — the tracking of fraud risk levels and exposures in a visual format that allows management to track the investigative, resolution, and corrective activities
- **Chain of Custody, Audit Trail and Documentation** – elements that enable the users to maintain a clear record of the analytics, and the steps performed and document the authenticity of the data, if needed
- **Case Management** — elements that support the workflow and business processes of fraud risk management and related analyses

Developing and Maintaining Data Analytics Processes and Procedures
Organizations receive the highest benefits when data analytics are integrated throughout the Fraud Risk Mmanagement Program. To do so, the entire team, including those specializing in data analytics, will be aware of the key elements of the fraud risk cycle, their own capabilities, and the common areas where analytics can be used to greatest effect.

Data analytics can potentially be used in every stage of the fraud risk management process: governance, assessing risk, implementing or strengthening control activities, reporting and investigating, and monitoring. The following are the typical elements, policies, and procedures that can be applied by the team under each principle, as appropriate.

- **Fraud Risk Management Planning** — A plan that covers the specific objectives, goals, strategies, and measures pertinent to each fraud risk management principle will serve as the overarching roadmap for applying data analytics in each phase of fraud risk management.
- **Fraud Risk Assessment** — Data analytics can look for known indications of fraud, outliers, and trend analysis. Other analytics can inform the assessment of fraud risk and identify needed control or investigative activities.
- **Controls Testing** — Data analytics can be used to test for compliance with established internal control rules. They can also identify cases in which risks exist for which no effective control has been established. When control weaknesses are identified, analytics can help quantify the exposure to improprieties.
- **Substantive Procedures** — Data analytics can often replace the need for sampling when they are used to analyze entire populations for transactions or balances to identify anomalies and problem areas.
- **Reporting Precise Findings** — When issues are identified, analytics can quantify the risks and exposures with a high degree of precision. For example, analytic tests might quantify that X purchase orders, with a total value of $Y, did not comply with company policies.
- **Continuous Monitoring** — Automated repeatable data analytics tests can enable a continuous or near real-time fraud risk monitoring process. This can provide timely analysis of changing fraud risks or identify when an audit or investigation is necessary and free up resources to focus on more complex high-risk areas requiring professional expertise. Once established, these analytics can operate with minimal additional resources until the process reveals an anomalous transaction.
- **Quality Assurance Review (QAR)** — A QAR process assesses the quality of risk assessments, audits, and investigations. This should include steps to assess whether analytics were applicable, whether they were used, and their effectiveness.
- **Maintaining Data, Queries, and Tests** — Elements that maintain the underlying data and the analytics themselves help avoid rework and contribute to an efficient fraud risk management process.
- **Maintain Access to Accurate Data** — Ensure that ongoing access to all information is in place, not just when the risk assessment is being performed. Identifying and obtaining the data to support fraud analysis and testing is frequently the most time-consuming part of the process. It requires not only a determination of the required data elements but also the ability to extract these from an IT system. Having an ongoing ability to access, develop an understanding of, and use the data prior to a potential risk assessment, audit, or investigation will greatly reduce the needed time and effort. Once data is obtained, validation confirms that the data is correct and complete before analytics are performed.

- **Develop and Maintain Queries to Extract Required Data:** Safeguard and maintain the extract queries. Important issues include maintaining security over access to data and managing the life cycle of the data from acquisition, through use, maintenance, and disposal.
- **Develop and Verify Analytics:** Use the results of risk assessments, audits, reviews, and investigations to validate the analytics and identify risks, control weaknesses, noncompliance, etc., that were identified by analytics. Data analytics tests range from relatively simple to complex. They can be intended for single time use to support a specific risk assessment, audit, or investigation or, alternatively, can be fully automated routines that run as part of a continuous monitoring process. As the level of complexity and automation increases, it is critical to design, develop, document, review, and maintain tests. Analytics should by reviewed and validated. Review and validation should evaluate test design; consider possible errors in test logic, assumptions, and coding; and validate the results of the analytics. Findings from the reviews help improve the program.
- **Identify and Re-run Analytics on a Regular Basis:** Use previous results or frauds to determine which analytics will be re-run to assess management action on risk mitigation activities; and the analytics to run on a continuous basis to assess existing, and identify emerging, fraud risks. An analytics library can make data analytics a sustainable, efficient, and effective. A well-managed and continually growing library of proven tests can often be applied in multiple areas.
- **Assess New or Emerging Risks and Data Sources:** Use risk assessments, audits, investigations, other reviews, and media reports to continually update the fraud risks and analytics to ensure that data sources, risk landscape, and analytics reflect the current risk environment. Fraud risks are reassessed on a periodic basis. Fraud risk indicators can be developed and measured to promote early identification of increased levels of fraud risk. Increased fraud risk may lead to a proactive investigation, catching fraud early. As illustrated in the next example, the fraud risk identification process starts with the business process objective and identifies the associated fraud risks and controls, analytics to test the controls, and the required data. The results are also linked back to the controls and fraud risks, so the mitigation actions are focused on the root cause of the risk — not just the symptoms.

  Reassessing and tracking the risk-analytic relationship helps identify which analytics were successful and cost-effective. They can be run on a periodic basis to keep the fraud risk assessment current. They can also be used to follow-up on management action plans and incorporated into a continuous fraud risk assessment process.

Below is an example of how the risk identification template can be used in assessing the effectiveness of controls.

To assist organizations in getting started with integrating data analytics into their fraud risk assessment or investigative work plans, a library of data analytic test examples are posted at acfe.com/fraudrisktools. These tests are organized by asset misappropriation, corruption, and financial misstatement classification categories and provide general guidance and examples for consideration in forensic data analytics efforts.

AP Business Objective: timely, accurate payment of approved invoice				
Risks	**Controls**	**Analytics**	**Data**	**Results**
• Duplicates • Fictitious • Inappropriate address changes • Bank account changes	• Vendor creation/ modification • Update log • Authorizations	• Duplicates • Blanks in key fields • Classify on "created by" • Vendor usage by clerk • Changes	• Vendor # • Created by • Entered by • Changes	• Duplicate vendors • Vendors with missing info • SOD and authorization issues
• Duplicates • Invalid invoices	• System controls over duplicate invoices • Invoice entry • Management review	• Duplicates • Invoice sequence	• Vendor # • Invoice # • Invoice date • Amount	• Duplicate invoices • Inappropriate payments or to wrong vendor
• Overpayments	• IR = GR = contract • Vendor creation/ modification	• IR <> GR or contract • Unusual payments to vendor	• GR and IR amount and quantity • Contract amount and quantity	• Pay more than contract

Results will dictate the need for strengthened or additional controls in specific areas.

APPENDIX D.2

Data Analytics to Support Fraud Risk Management

From general ledger accounting systems to network security, email, and social media, data is the all-encompassing backbone of modern organizations. Understanding complex data sets from multiple sources within a business is important, especially when addressing fraud risk management or responses to regulatory demands, when engaging in an investigation, or when trying to prevent the need for one.

Fraud Risk Assessment

To develop a data analytics plan related to fraud risk, an organization first performs a fraud risk assessment, as described in Chapter 2 of this Guide. In doing so, it uses several techniques and approaches to support the identification and assessment of fraud risk. In addition to brainstorming, organizations examine fraud risks or vulnerabilities, identify critical controls and consider their effectiveness, and identify key data elements that support business processes, such as accuracy, timeliness, and authorization, to determine if there is proper protection.

This appendix provides guidance on the application of these techniques and approaches to fraud risk assessments as they relate to data analytics. The appendix also provides several practical examples of analytics procedures. Identifying fraud risks or vulnerabilities is integral to this process and critical to an organization's data analytics framework.

Examination of Fraud Risks

Organizations devise data analytics strategies for identified fraud risks. Use of a simple template like the one completed below helps identify and assess fraud risks and the appropriate related data analytics planning.

Detection techniques employ data analytics to examine trends, perform recalculations, and look for anomalies. For example, the assessment of risk related to separation of duties involves developing a table that determines who is performing which duties and then looking for instances in which the same person has performed incompatible duties (e.g., receipt of goods and entry of invoice).

An example of a fraud risk assessment follows:

Potential Risk Factor*	Typical Issues	Detection Strategy
Financial misstatement	• Unrealistic performance measures compared to industry peers • The timing of revenue, shipping, returns, and discounts out of line with the appropriate reporting period • The timing of expenses out of line with the appropriate reporting period • Unusual spikes or capitalization charges	• Revenue analysis, including assessing trends in production or sales figures and looking for downward adjusting entries in the period after bonuses are awarded • Period comparisons • Management overrides of controls as evidenced by journal entries initiated by senior managers • Establishment of or unusual variations in accounting reserves
Misappropriation of assets (digital and physical)	• Unauthorized access to sensitive data • Data leakage to third parties or unauthorized individuals • Internally deployed cyber attacks • Theft of physical assets • False or inflated vendor invoices • Contract and bidding fraud • Ghost employees • Fictitious vendors	• Review of access controls and information security • Analysis of network traffic and access activity • Review and trending of disbursement data • Check for management overrides of controls • Pattern and link analysis to identify hidden relationships or conflicts
Bribery and corruption	• Employee/vendor conflicts of interest • Kickbacks or gross-ups disguised as vendor payments • Excessive meals, travel, or entertainment expenses or exotic locations • Unusual margins or payments to third-party distributors or agents	• Match employee/vendor addresses, phone, etc. • Analyze accounts payable or employee expenses for potentially improper payments • Analyze high-risk GL or subledger accounts • Analyze third-party setup and due diligence processes

*Refer to ACFE's Fraud Tree for a more comprehensive view of fraud risk factors to consider.

Data Analytics Framework

The scope of this Guide is not intended to be all-inclusive with respect to data analytics considerations. However, a useful data analytics framework describes five distinct phases involved in establishing a meaningful data analytics framework. These phases include assessing areas of inherent fraud risk, identifying control weaknesses, supporting any investigations, and reporting and follow-up on areas of identified indicators of fraud. As introduced in Chapter 3, the five phases of this framework are as follows:

Analytics Design	Data Collection	Data Organization & Calculations	Data Analysis	Findings, Observations, & Remediation
• Identify risks based on industry and company-specific knowledge • Map risks to appropriate data sources and assess availability • Develop work plan and define analytics and procedures • Define engagement timeline and deliverables	• Work with information technology personnel to map identified tests to relevant data sources • Assess data integrity and completeness • Extract, transform/normalize, and load data into the analytics platform • Validate that data has been loaded completely and accurately	• Execute on the analytics work plan and conduct necessary mathematical procedures • Modify analytics as appropriate based on data received, data quality, and user feedback • Consider integrating advanced analytics procedures such as text mining, statistical analysis, and pattern/link analysis	• Evaluate initial analytics results • If possible, develop scoring model and prioritize transactions or entities based on multiple risk attributes • Tune the model as needed to refine results for relevancy	• Request supporting documents and/or validate as available • Determine sample selections or triage/escalation procedures • Develop remediation and/or investigative plan • Escalate findings as appropriate and track dispositions

Phase I: Analytics Design

This phase encompasses identifying risks, mapping those risks to available data sources, developing and planning data analytic procedures, and defining the timeline and deliverables.

Identify Risks Based on Industry and Company-Specific Knowledge

This phase focuses on asking the right questions. Rigorous anti-fraud brainstorming can be an effective tool to identify fraud risks up front. Identifying the fraud risks drives the use of data and technology, rather than the other way around. The human element, such as knowledge of the industry and company risks and the experience of the team on the project, helps ensure that the data analytics properly link to the risk assessment.

Useful considerations include:

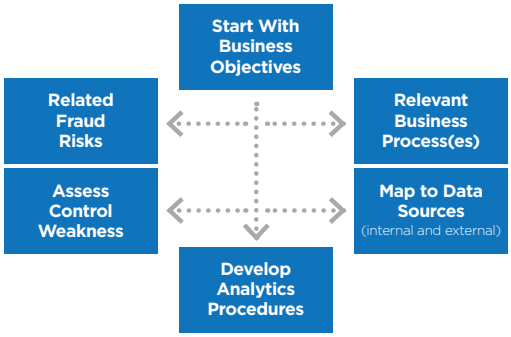
- **Business process** — What business processes pose a high fraud risk? Often, high-risk business processes include the sales (order-to-cash) cycle and payment (procure-to-pay) cycle. Other high-risk processes include payroll, accounting reserves, travel and entertainment, and inventory.
- **Accounts** — What are the high-risk accounts within the business process that could identify unusual account pairings (e.g., a debit to depreciation and an offsetting credit to a payable — a "**cookie jar reserve**")? What accounts have vague or open-ended "catch-all" descriptions, such as "miscellaneous," "administrative," or blank account names?
- **Preparer** — Who recorded or authorized the transaction? Posting analysis or approver reports help detect unauthorized postings or improper segregation of duties by looking at the number of payments by name, minimum or maximum amounts, sum totals, or statistical outliers.
- **Time series** — What is the time period of the analysis? Analyzing the transaction activities over time can identify spikes or dips in activity, such as before and after period-ends or weekends, holidays, or off-hours activities.

Map Risks to Appropriate Data Sources and Assess Availability

Not surprisingly, the use of data analytics requires access to data. Most often, that data is internal to the organization. However, external data, such as social media, news feeds, cyber events, and information in the public domain can be very helpful. It is not always easy to identify the relevant data set, define the data requirements, and obtain access to the required data. In addition, the integrity of the data, the reliability of the analysis, and the interpretation of the results are very important.

The following graphic illustrates a high-level process framework for designing analytics procedures. By starting with the business objectives, one can map to the related fraud risks that can hinder achieving those objectives. Those fraud risks are most often aligned to a relevant business process or multiple processes. After identifying the business process, assess the control weaknesses of that business process, then map to relevant internal and external data sources. Selection and development of analytics procedures occurs only after identification and documentation of these factors.

Assessing Controls in Areas of High Fraud Risk



The design of analytics for the procure-to-pay cycle should not be limited to a mere "accounts payable" analysis. Accounts payable is merely a data source. In designing analytics, it would be better to think of a "business-spend analysis" for which the business objective is to reduce the fraud risk of potentially improper or corrupt payments. With this mind, the focus shifts from what is available only in accounts payable, to a more robust view of what is an improper or corrupt payment, which could include consideration of the vendor and employee master data sets for conflicts of interests; the due diligence performed on the third parties receiving the payments; or any adverse news, social media, or sanctions related to the third parties.[21]

Develop Work Plan and Define Analytics Procedures, Timeline, and Deliverables

Preparing the work plan, procedures, timeline, and the nature of the deliverables are the key components of this phase. Sometimes, an analytics work plan can span just two or three weeks to conduct a problem-focused analysis. Other times, a work plan is part of a broader Fraud Risk Management Program that is a longer-term project or an ongoing business process. It is important to understand and set realistic task, resource, and timeframe expectations so that management can evaluate the cost of the analysis weighed against the significance of the fraud risk addressed.

In addition, providing managers and project sponsors with deliverable examples, case studies, reports, or analytics dashboards using sanitized or hypothetical data can help set proper expectations and gain commitment and resource allocations for the work.

Phase 2: Data Collection

Data collection encompasses working with IT personnel to map planned tests to data sources, assessing the completeness and integrity of the data, extracting and loading the data into the testing platform, and validating that data have been loaded completely and accurately.

Map Identified Tests to Relevant Data Sources

Once the data analytics team identifies the planned analytics, it works with the custodians of the necessary data sources and requests certain extracts or copies for use in the analysis.

Often, the custodians of the necessary data are the company's IT professionals or business line personnel. Custodians also can include outside third parties such as business information services, data hosting providers, or third parties connected to the company's supply or customer chain.

Assess Data Integrity

It is useful to have someone on the team who is familiar with the data structures and data types so the team can properly request what needs to be extracted as well as the data format to help ensure proper data extraction, validation, and loading into the analysis platform. In many organizations, it is possible to utilize data sources in a secure, read-only mode without requiring that they have to be copied to a separate system. Data extraction procedures also can be automated in some instances to refresh the data on a regular basis.

Extract, Transform, and Load Data into the Analytics Platform

In addition to extraction and loading, data sets must often be normalized or transformed so that the data is in a proper format for analysis. The principal concern related to this step in the process is ensuring that data loaded into the analytics platform remains complete and accurate. To this end, it is important to use control totals of transactions and characters to provide assurance that no transactions are omitted or altered. After attaining that micro-level of assurance, it is appropriate to perform further macro-level validation steps.

Validate That Data Has Been Loaded Completely and Accurately

Upon receipt of the requested data, the team performs the following data validation and quality checks:

- Confirm that the data format meets the data request requirements
- If data is not in the expected format, check other fields, such as monetary fields, date and time, text encoding, and delimiters
- Obtain source data with control totals and reconcile results to confirmed or audited data sources, such as trial balance for the period
- Visually inspect that date ranges of data match the project scope

[21] David Coderre in *Computer-Aided Fraud Prevention and Detection: A Step-by-Step Guide.*

- Confirm that all expected fields are present in the data
- Visually inspect the beginning and end of the data source to check field consistency such that no data has shifted during export
- Visually inspect the maximum length of fields to determine truncation issues
- If applicable (or reasonably available), trace account totals back to audited financial statements or to the trial balance
- Maintain a data-tracking log of files received as part of the documentation

Phase 3: Data Organization and Calculations

This phase involves carrying out the analytics work set forth in the plan and considering additional tests or procedures as new information arises.

Execute on the Analytics Work Plan and Conduct Necessary Mathematical Procedures

In this phase, the team organizes the data into a centralized platform or data-base from which it is possible to execute certain mathematical and operational functions consistent with the analytics work plan.

Modify Analytics as Appropriate Based on Data Received, Data Quality, and User Feedback

Often the data requested, validated, and loaded into the system for analysis comes with certain limitations that may require modification to the analytics work plan or listing of testing procedures. For example, certain data fields might be missing, free text payment descriptions might be incomplete or non-descriptive, or certain data simply just does not exist. In other cases, data may be too cost-prohibitive to acquire relative to the significance of the fraud risk being analyzed. In these circumstances, flexibility is key. Tests might have to be redesigned, certain assumptions might have to be made, or certain tests may need to be eliminated altogether.

Sometimes it is better to run analytics on 80% of the available data, rather than to not run them at all. In those circumstances, it is important to document and communicate the limitations to the project sponsors and to include reasonable explanations for the modifications being made.

Case Example Using Summary Statistics and Sorting

Management had concerns about prices customers were being charged for products, so the auditors calculated the ratio of the maximum sales price to the minimum sales price for each product. (A ratio that is close to 1.0 means that there is little variance between the highest and lowest prices charged to customers. However, a large ratio could be an indication that a customer was being charged too much for the product, or that a customer was not being charged enough.)

The analysis identified numerous instances of products with ratios of 2.0 or higher.

Product Line	Max	Min	Ratio
Product 1	266	127	2.09
Product 2	286	283	1.01
Product 3	68	34	2.00

For example, the analysis showed that products 1 and 3 had large differences in price between the minimum and maximum (ratios of 2.0 or higher), whereas product 2 had a small variance in prices (ratio of 1.01). The transactions for products with ratios greater than 1.5 were examined to determine if the proper pricing had been used. The result highlighted a fraud in which a salesman was manipulating prices in exchange for kickbacks.

Integrating Analytics Procedures

This phase might include a variety of analytics procedures, including the following examples listed from relatively easy to more sophisticated. More detailed analytics procedures are further described in Appendix D-3.

- Sorting data from highest to lowest, or vice versa, or segmenting/stratifying data by account types.
- Generating summary statistics on the data (min, max, average, mean, sums, etc.)
- Performing customized queries, such as matching, joining, filtering, and other rules-based tests, on certain fields in the data to identify certain policy or segregation issues
- Verifying proper separation of duties through a simple pivot table that highlights instances in which an individual has performed incompatible duties

Phase 4: Evaluation of Data Analysis

After performing initial tests, the analytics team analyzes and prioritizes results and considers whether to refine the tests to yield more meaningful or easy-to-evaluate results.

Evaluate Initial Analytics Results

With the test plan, data sources, and algorithms in place, the next step is to analyze the data in line with the fraud risk work plan. In the accounting and anti-fraud profession, traditional analytics outputs are often spreadsheet-type outputs or static graphics, such as a pie or line chart. However, because business intelligence and visualization technologies have vastly improved, users can "interact" with the data in ways that transcend the use of simple rows and columns. Therefore, the user can better interrogate the data from multiple dimensions or perspectives.

Develop Working Model and Prioritize Transactions or Entities Based on Multiple Risk Attributes

As described further in Appendix D-3, companies also can utilize risk-scoring techniques when looking for fraud risk areas in their data. Risk scoring techniques allow for a more complete assessment of the data because they allow analytics to be run on the entire population (100% testing), rather than just a sample. Risk scoring also allows for a systematic and repeatable process for prioritizing transactions for further evaluation.

Fine-Tune the Model as Needed to Refine Results for Relevancy

Finally, the analytics team fine-tunes the analytics output. Anomalies may be identified, issues may be surfaced, or patterns may appear that require further drill down or investigation into the data. Often, test results produce output that is too voluminous to facilitate easy or meaningful analysis. By studying the initial output, the team can add filters to the results to eliminate some of the irrelevant volume. Further, the team may need to execute new tests or procedures based on the initial results. Flexibility and creativity in adjusting the analytics helps facilitate ad-hoc requests or additional hypothesis testing.

Phase 5: Findings, Observations, and Remediation

Once the data analysis has produced results, the team carefully considers the findings and observation from the testing and considers an appropriate response. This may include additional testing, investigation of potentially fraudulent conduct, remediation of process or internal control deficiencies, reporting results, and tracking dispositions.

Request Supporting Documents and/or Validate as Available

In the findings, observations, and remediation phase, the goal is to refine the analytics output into some form of actionable decision that is meaningful to the business objective. This actionable decision could be to remediate a control weakness, to initiate an investigation, or formulate a business conclusion. In most cases, the results of the analytics output do not dispositively provide that a fraud or malfeasance has taken place. Rather, analytics typically point to anomalous transactions. Further investigation, which may include interviews or substantive testing, takes place to gather supporting documentation and other evidence and develop findings, as discussed in Chapter 4 of this Guide.

Determine Sample Selections or Triage/Escalation Procedures

From a governance perspective, it is also helpful to have defined triage or escalation procedures in place to ensure that issues are not missed and that items are properly followed up and resolved in a systematic way. Case management tools may be utilized to manage workflow and assign tasks to an investigative team, which may include inside or outside counsel. Having a defined process identified to properly triage the analytics output helps to ensure that minor issues are not burdening management and that major issues are properly addressed.

Develop Remediation and/or Analytics Investigative Plan

When fraud is suspected — either because of data analytics or because of allegations, a detailed fraud investigation plan helps ensure that all relevant aspects of the possible fraud are determined.

For the investigation plan, we recommend referring to Chapter 4 of this Guide, particularly as it relates to the data analytics point of focus.

Escalate Findings as Appropriate and Track Dispositions

Finally, as issues are identified and remediated, they are escalated appropriately and tracked over time by category. This process is not only helpful from a compliance, regulatory, or legal perspective, but also, if there is outside scrutiny of the issue, it helps demonstrate key performance indicators and return on investment from the analytics initiatives. Case management software tools can help organize and report on work performed, key findings, recoveries, and remediation activities taken.

APPENDIX D.3

Data Analytics Techniques

Data Analytics Techniques for Fraud Control Activities

You can't monitor what you can't measure. Integrating data science and analytics resources into traditional anti-fraud monitoring functions provides the organization with better business transparency, which in turn can improve corporate culture, reduce the instances and severity of fraudulent events, and, in the end, improve business performance. A data-driven, coaching, and continuous monitoring approach (versus an authoritative, investigative, audit approach) is one of the best ways to establish a culture of integrity. Some of the data analytics techniques discussed in this appendix can be used as additional or enhanced fraud control activities to mitigate residual fraud risks that were identified during the fraud risk assessment.

While there are literally thousands of different data analytics approaches and tests, there are a number of common approaches and techniques that can be considered as part of a company's fraud control activities.

Common Analytic Tests Linked to the Major Categories of Occupational Fraud

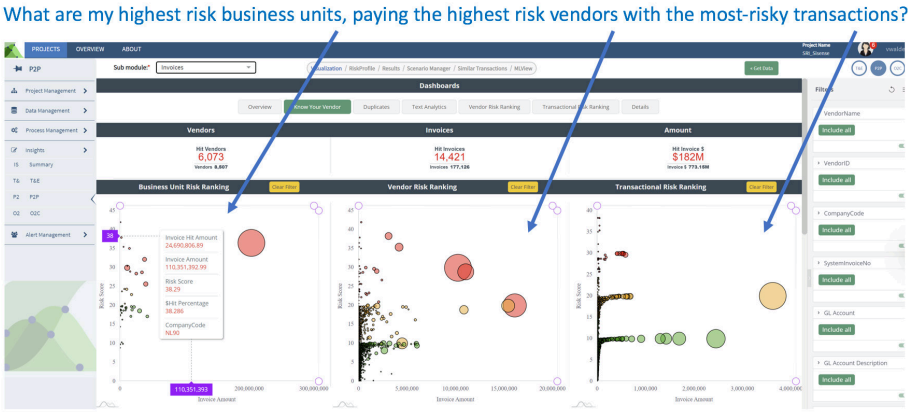
To assist organizations in getting started with integrating data analytics into their fraud risk assessment or investigative work plans, a library of test examples can be found at acfe.com/fraudrisktools. These tests are organized by asset misappropriation, corruption, and financial misstatement classification categories and provide general guidance and examples for consideration in forensic data analytics efforts.

- **Big fraud risks require big data thinking —** This involves asking more robust anti-fraud questions by combining multiple internal and external data sources. Big data thinking starts with asking the right business risk questions and focusing on the highest risks first. The highest fraud risks are in the upper right-hand corner of a fraud risk assessment heat map — high likelihood and high significance (see Chapter 2). Fraud risks should not start with a single data source — for example, let's not say "We want to do an accounts payable review or an employee travel and expense (T&E) review as part of our fraud preventive and detective activities. That is a myopic view that only considers one data source (e.g., accounts payable or employee T&E) and is destined to yield mediocre results. Instead, start with the right business questions. If vendor risks such as corrupt or improper payments to third parties, conflicts of interest, or payments to government officials are in the top fraud risk category, for example, then clearly start with that fraud risk issue. Before jumping into data sources, next brainstorm and write down what fraud risk tests or analytical procedures to perform if all the information (both internal and external) is available. This creates big data thinking.

  Only then, map those fraud risk tests or analytics procedures to the appropriate data sources. Of course, accounts payable will be an important element for running a vendor risk review or monitoring — but it is not the only data source. Other sources might include the third-party due diligence that was done on the vendor during setup, external adverse media on any vendor, vendor master details, or contractual information. The same goes for an employee T&E review. It's not a T&E fraud risk review, it's an employee fraud risk review. T&E is a data source, but employee risks can come in the form of conflicts of interest (compare employee information to the vendor master file), data leakage or security, sales performance and kickbacks, abusive free goods or samples, and so forth. In line with this big data concept, techniques that incorporate multiple, disparate data sources to proactively identity, analyze, and monitor emerging risks can sometimes be referred to as "risk screening." In the end, its best to keep in mind that the bigger the risks, the more robust you should be in thinking about your data sources to provide intelligent insight.

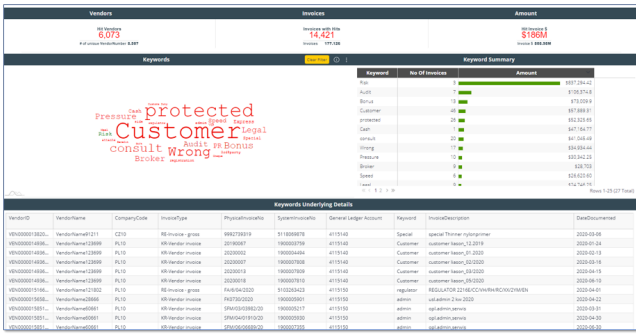
- **Transaction risk scoring —** The concept of transaction risk scoring can be a game-changer to anti-fraud professionals using data analytics. Traditional approaches or fraud control procedures would look at one fraud risk test in isolation — such as a payment transaction with a "date paid" date before the "invoice generated" date — with no context as to the many other tests that can be run on that same transaction. The result of this approach is often too many false positives. Instead, consider a transaction risk scoring approach where multiple risk factors are considered at the same time to essentially "risk score" a transaction. With a transaction being the lowest common denominator, this allows associating the highest risk transactions with vendors, employees, or customers. With knowledge of highest risk vendors, employees, and customers, then roll it up further to the highest risk business units or geographies and generate a fraud risk heat map that is based on the roll-up of all the riskiest transactions. For example, don't just show payments with "date paid" before the "invoice date," show the top 10 or top 25 riskiest transactions out of the entire population that hit on the most risk triggers. As an example, showtransactions that: (1) were paid before they were invoiced, (2) were over $10,000, (3) were paid in round dollars (indicative of cash or some sort of service rather than goods exchanged), and (4) contained a sensitive keyword hit such as "special payment," "facilitation payment," or "gift."

- **Data visualization —** Data visualization tools are mainstream across all aspects of business, including the fraud risk management function. When looking for anomalous patterns and relationships, taking a "spreadsheet view" in rows and columns is not as effective as looking at the same data in an interactive dashboard-type view. Organizing data in tables, whether in a spreadsheet or using more scalable data-base or data warehouse tools, is still necessary. That said, the output from queries, statistical analyses, and risk scores are better viewed in a dashboard-type interface that is supported by the underlying tables and databases. Data analytics professionals and managers alike appreciate the ease and insights gained from presenting the data visually. An example of a data visualization dashboard follows:



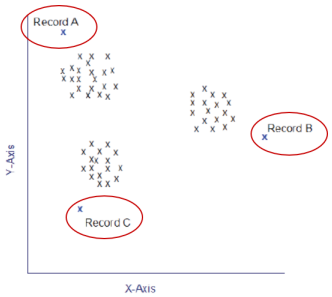
- **Text mining to find corrupt intent —** When entering a payment description, what people use to describe a potentially improper or fraudulent payment, sales entry, customer expense, gift, or entertainment activity is quite telling. Words like "friend fee," "help payment," "respect fee," "volume contract facilitation," "timing adjustment," "miscellaneous," or "customer incentive" have all been used to describe bribes, abusive expenses, or conflicts of interests. Individually, they are suspicious, but when grouped with their respective transaction details such as dollar amounts, text mining can be an extremely effective preventive and detective tool. A detailed explanation of the science of text analytics and linguistic analysis is beyond the scope of this appendix. However, two techniques are most common and useful:

  - **Keyword search —** Keyword search is the same type of search that can be performed in MS Office tools, on the internet, or during an email review. The most common type of keyword search is a Boolean keyword search that allows the user to combine words and phrases using the words AND, OR, NOT, NEAR (known as Boolean operators). In any keyword search, the user provides fraud risk terms that might be in the data. While keyword searches are often effective, this "supervised" approach inherently injects bias into the analysis given that the user does not know the code words or terms used in the data. The fraud risk terms are selected based on the user's knowledge of the business and the fraud risk issues at hand. The other, sometimes more effective approach is using statistical text mining techniques.[22]
  - **Text mining —** The word cloud below is an example of a text mining technique where the word "customer" is highly frequent (where the size of the font indicates the total dollar amount of transactions or frequency in the journal entry or document description. Normal words like "customer" or "invoice" would be expected terms used to describe payments, but words such as "wrong," "pressure," or other less expected words in a smaller font can uncover potentially improper or fraudulent payments.

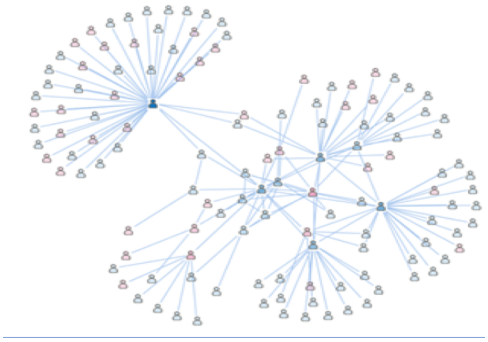


[22] Text mining: The process of extracting information from collections of textual data and utilizing it for business objectives. https://www.gartner.com/en/information-technology/glossary/text-mining.

- **Statistical analysis —** In addition to concept searching and unsupervised learning statistical techniques, other advanced statistical analysis techniques can also be relevant. Some particularly useful statistical analysis techniques include:
  - **Statistical anomaly detection identifies unusual cases, or outliers, that do not conform to patterns of "normal" data —** For example: In the graph below, vendors A, B, and C would be considered anomalous based on whatever categorical variable (spend, location, invoice formatting, recurring payments, contract terms, etc.) did not match (or was not statistically similar) to other transactions. This is a good technique for identifying unusual payments or sales activities as well as manual journal entries that do not fit the norm. Since records A, B, and C are outliers, they would be good candidates for selection and deeper dive reviews.



  - **Pattern and link analysis seeks to identify hidden relationships between entities —** Whether that entity is a customer, vendor, or employee, the software will seek to find commonalities such as same or similar physical addresses, matching bank account numbers, common communication patterns, and so forth. This technique is also a good unsupervised technique, because it does not require the user to pre-define what a match looks like. When set up properly, any record in a data-base could contain matching (or highly similar) content to any other record in the data-base, thus linking the entities (again the customer, vendor, or employee) to those respective transactions which may not have been previously known. The figure below is an example of the results of a social network analysis.



- **Artificial intelligence (AI) and machine learning —** Gartner Research defines AI as "applying advanced analysis and logic-based techniques, including machine learning, to interpret events, support and automate decisions and take actions." In an anti-fraud context, AI can be quite powerful. For example, when certain known fraudulent transactions are identified, the attributes of those transactions (such as the dates, the amounts, the employee entering those transactions into the accounting system, the customer or vendor, the geographic location, free-text payment description, among any other field in the data-base) can be modeled using machine learning to find statistically similar (more-like-this) transactions to speed up review and decision making. For example, in a hypothetical revenue recognition investigation where the investigator needs to understand the potential universe of potentially improper sales transactions, a small subset of bill-and-hold schemes that were initially identified from one customer totaling $15,000 is modeled using machine learning techniques (primarily multi-variable regression). When that training set of known fraudulent transactions is fed into a model of all the sales transactions for the past two years, the machine learning algorithm identified 2,500 statistically similar transactions that represented over a dozen customers and $550,000 of potentially improper transactions.

  AI can also be applied to reduce human labor in the form of robotics process automation (RPA) techniques. A macro in MS Excel is a form or RPA. However, today's tools are far more sophisticated and can automate processes across multiple software applications to provide a vast array of data loading, data validation, and reports on an automated basis which can save time and money. Any process that involves repeating the same mouse clicks and/or moving files from one place to another may be an opportunity for RPA. While not directly attributable to fraud risk itself, RPA automates the data gathering and, in many cases, the human rules-based decision making (such as in a Boolean search), to enable a cost-effective continuous monitoring platform to improve fraud prevention and detection.

  Chatbots are another form of AI that can be quite effective for communicating fraud risk policies and managing helplines. Rather than calling compliance and speaking to humans, for example, chatbots are being customized for companies on mobile apps or computers where employees can ask sensitive questions about compliance, and the chatbot can answer based on the topic. In a hypothetical example, the fraud risk management team at a large company with over 100,000 employees was surprised to learn that the number one most frequently asked (or searched) topic by employees using the chatbot was, "What is a conflict of interest?"

The above examples are not comprehensive. This Guide's authors encourage users to include multiple skills sets, beyond anti-fraud, accounting, or legal, on the fraud risk management team. Including data science, information technology, information security, sales, or product members as well as human resources to collaborate on fraud risk areas and related mitigating analytics controls will result in a more robust use of data analytic tools.

Leverage Existing In-house Resources

As a final point, if your organization has a marketing department, finance department, information technology team, or some other business function where the analysis of data requires them to utilize business intelligence, data warehouse, or data visualization tools to help them make decisions, you may be able to leverage what's already in place at your organization. Whether those resources require major or minor modifications is typically based on the nature and complexity of the business. However, anti-fraud professionals may quickly discover there are some "quick-hit" wins and/or cloud-based solutions that other business departments have led, where existing business technologies and processes can be easily modified to provide detailed insight into a particular fraud risk area.

Case Examples

From a March/April 2022 article in *FRAUD Magazine* authored by Vincent Walden, the following are some practical examples of how some organizations are improving and updating their compliance and fraud risk management programs building off of existing programs and integrating some of the aforementioned analytical techniques:

- The vice president of internal audit at a manufacturing company and her team use scripting (i.e., a programing language that automates certain tasks) and other self-operating tools with their financial accounting/enterprise resource planning (ERP) system to refresh monthly and quarterly data on all global procure-to-pay and travel and expense (T&E) spending. Hosted on a secure, third-party cloud-based analytics platform, their fraud risk management and compliance monitoring system assesses and monitors hundreds of thousands of payments each month, and ranks thousands of vendors and employees from highest to lowest risk based on over two dozen risk criteria.
- The chief human resource officer at a national skilled home-healthcare, hospice care, and personal care services organization uses scripting and automation tools to gain better insights into her organization's employee payroll base by integrating over 1,200 distinct payroll files across several years and business units, representing the payroll activity of over 25,000 full- and part-time employees. Working with her IT department and an outside consulting firm, she leveraged existing business intelligence software tools already in use in her organization to build dynamic, risk-scoring, and anomaly detection dashboards that flag payments to terminated employees, statistically anomalous payments, potential overtime abuses, repeated hiring and termination patterns, and off-cycle disbursements, among many other data-driven tests.
- On a larger scale, an international beverage company uses in-house resources across its IT, data science, finance, and legal departments to improve transparency across all of its third-party vendors, employee travel and entertainment expenses, and several other key business processes through its proprietary platform.

APPENDIX E

Fraud Risk Assessment Example

This hypothetical example is for illustrative purposes and focuses on some potential schemes that might be documented during an organization's fraud risk assessment process. An actual fraud risk assessment would often be more extensive and have more detailed and organization-specific documentation, especially for large or complex organizations. This fraud risk assessment consists of four sections: (A) Financial Reporting, (B) Non-financial Reporting, (C) Asset Misappropriation, and (D) Illegal Acts/Corruption. To facilitate review, risks in each section are listed in descending order of Residual Risk and then by Likelihood and Significance.

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Section A. Financial Reporting							
FR1. Inappropriate journal entries	Medium	High	General manager and accounting and finance staff at the operating unit level and/or CFO, accounting, and finance staff and senior executives (e.g., CEO and COO) at the head office level	Established process for consolidation Established, systematic access controls to the general ledger Standard monthly and quarterly journal entry log maintained Review process in place for standard entries and non-standard entries subject to two levels of review with particular emphasis on quarter-end or year-end transactions and those transactions that reversed in the following month	Tested by IA — some findings Tested by IA — no findings Tested by management	High — Risk of management override of internal controls to misstate financial results by making journal entries	Data analysis of journal entry population by IA for: • Unusual DR/CR combinations • Late entries to accounts subject to significant judgments and estimates • Indications of journal entries being approved or entered by persons not usually involved, e.g., by more senior management or others using special or unauthorized system access
FR2. Revenue recognition — side letters/agreements with concessions, e.g., extended payment terms, price reductions, rebates, unusual sales/marketing support funding for dealers, distributors, or retailers	Medium	High	Salespersons, sales management Potentially senior executives (e.g., CEO and COO), legal and accounting and finance	Annual training of sales and finance personnel on revenue recognition practices Quarterly signed attestation of sales personnel concerning extra contractual agreements Internal audit confirming with customers that there are no other agreements, written or oral, that would modify the terms of the written agreement Testing of purchase orders to shipping documents and cash receipts for transactions entered into at or near the end of a quarter or year	Training deemed adequate Tested by IA — no findings Strong and effective	High — Risk of management override of internal controls leading to significant/material misstatement of revenue and net income Medium - Lax enforcement of training requirement may lead to isolated examples of improper revenue recognition by lower-level personnel	Disaggregated analysis of sales, sales returns, and adjustments by salesperson Add to all purchase orders, invoices and contracts a statement about the organization's ethics and how to report misconduct Have sales personnel affirm annually that they have not modified terms of sales contracts by allowing concessions or altering payment terms
FR3. Revenue recognition — delivery of product prior to customer's requested delivery date or prior to receipt of customer's order	Medium	High	Sales and shipping Potentially senior executives (e.g., CEO and COO)	Systematic matching of sales order to shipping documentation; exception reports generated	Tested by management — no findings	Medium — Risk of management override of internal controls to initiate early shipment and revenue recognition for significant sales	IA will increase cut-off testing
FR4. Revenue recognition — partial shipments	Medium	High	Sales and Shipping Potentially senior executives (e.g., CEO and COO)	Systematic shipping documents manually checked against every shipment Systematic matching of sales order to shipping documentation; exception reports generated Customer approval of partial shipment required prior to revenue recognition	Tested by management — no findings	Medium — Risk of management override of internal controls to initiate partial shipments and record revenue on them despite not having customer approval for partial shipments	IA will increase cut-off testing Analytics testing of patterns in partial shipments (e.g., same salesperson, same customer)
FR5. Revenue recognition — recording revenue for items shipped after books closed for period end (aka late shipments)	Medium	High	Shipping Potentially sales management, some sales persons, accounting and finance, and senior executives (e.g., CEO and COO)	Integrated shipping system, linked to invoicing and sales register Daily reconciliation of shipping log to invoice register Required management approval of manual invoices	Tested by IA — no findings Tested by management — no findings Tested by IA — no findings	Medium — Risk of management override of internal controls to record as sales items that were not shipped until after the end of the accounting period	More frequent cut-off testing by IA Analytics to identify items with shipping dates after period close

For column explanations, please go to page 95.

Fraud Risk Assessment Example

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Section A. Financial Reporting							
FR6. Revenue recognition — holding books open to record in the current period revenue from sales made in the next period	Medium	High	Accounting and finance, senior executives (e.g., CEO or COO), and sales management Potentially sales persons	Standard monthly close process Reconciliation of invoice register to general ledger Established procedures for shipping, invoicing, and revenue recognition Established process for consolidation	Tested by IA — no findings Tested by management — no findings Tested by IA — no findings Tested by IA — no findings	Medium — Risk of management override of internal controls to hold the books open	Data analytic identification and testing of late journal entries Sales cut-off testing by IA
FR7. Manipulation of liabilities/ expenses — unrecorded vendor invoices	Medium	High	Accounting and finance Potentially senior executives (e.g., CEO and COO)	Vendors are instructed to send invoices only to the centralized accounting function where they are logged into A/P system upon receipt and held in a suspense account as "pending approval" until authorized by the relevant department Department heads and accounting review the nature/value of pending invoices at period end to help ensure proper cut-off	Tested by IA — some invoices for marketing, consulting, and legal services were sent to department heads and not recorded until they were later approved	Medium — Risk of management override of internal controls to defer recognition of current period liabilities/ expenses into next period by not processing invoices from certain vendors, for select transactions, or for a particular period (not necessarily at year-end)	IA will use data analytics to identify and test major invoices processed in non-standard manner to identify potential recording in wrong period Accounting function will check each quarter-end with the heads of marketing and legal departments and with CEO to help identify major invoices not recorded in A/P system
FR8. Revenue recognition — manipulation of secondary revenue streams e.g., service and support revenue	Low	Medium	Sales and accounting and finance Potentially senior executives (e.g., CEO and COO)	Signed customer contract documentation is required to record service/support revenue	Tested by IA — no findings	Medium — Risk of management override of internal controls to create fictitious sales or to "front load" revenue recognition in secondary revenue streams	IA will implement data analytic tests for unusual trends and transactions
FR9. Revenue recognition — backdating sales agreements	Medium	High	Sales persons, sales management Potentially accounting and finance, legal, and senior executives (e.g., CEO or COO)	A clear revenue recognition policy and training for all sales persons, sales management, and accounting and finance personnel involved in accounting for sales CEO and VP sales both set a clear and strong tone about making sure revenue recognition conditions are met before sales are booked as revenue — violators are disciplined, including termination for "serious" offenses, e.g., lying to management Well-controlled sales contract administration system Sales management monitors transactions in sales contract system to help ensure compliance. They give extra scrutiny to significant sales booked in the last two weeks of each quarter	Tested by IA — no findings	Low	None required due to low residual risk Existing testing of fraud controls is sufficient
FR10. Revenue recognition — channel stuffing	Low	Medium	Sales persons and sales management Potentially accounting and finance, legal, and senior executives (e.g., CEO or COO)	VP Sales has established a clear policy requiring written pre-approval for all sales in excess of 3 months' usage and which exceed $1 million Sales managers review each salesperson's sales figures by customer Senior sales management reviews sales figures for each location/ business unit Accounting and finance function performs analytical review on sales figures and compares to budget and projections	Tested by IA — no findings	Low	None required due to low residual risk Existing testing of fraud controls is sufficient

For column explanations, please go to page 95.

Fraud Risk Assessment Example

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Section A. Financial Reporting							
FR11. Disclosures — improper or inadequate disclosures of material facts, circumstances and events	Low	Medium	Senior executives (e.g., CEO and COO), accounting and finance, and legal	CFO and controller confer with senior management and legal to ensure all appropriate disclosures have been made Periodic reviews by outside counsel, sign off by senior management and CFO and controller Review by disclosure committee of the board of directors	Tested by IA — no findings	Low — Risk of management override of internal controls over disclosures, e.g., to prevent timely disclosure of: adverse drug trial results, failure to win a key contract, or indications of defective product with liability consequences	None required due to low residual risk
FR12. Revenue recognition — manipulation of bill-and-hold arrangements	Low	Low	Sales and accounting and finance Potentially senior executives (e.g., CEO and COO)	None required due to low inherent risk	N/A	Low	None required due to low residual risk
FR13. Revenue recognition — roundtrip transactions	Low	Low	Sales and accounting and finance Potentially senior executives (e.g., CEO and COO)	None required due to low inherent risk	N/A	Low	None required due to low residual risk
Section B. Non-financial Reporting							
NF1. Quality — material testing results altered	Medium	High	Production, vendors, and internal QC personnel Potentially also sales management and sales personnel for affected customers and senior executives (e.g., CEO and COO)	Independent sample testing	Immaterial negative results	High — Bait/switch, Collusion, kickbacks, or management override of internal controls to alter material testing results for raw materials, components, or final products to avoid demonstrating violation of key contract provisions	Conduct more frequent testing using larger samples Add to all purchase orders, invoices, and contracts a statement about the organization's ethics and how to report misconduct Analytics to track trends in returns due to quality issues
NF2. Compliance — environmental, health and safety reporting	Low	High	Operating unit leaders, production, warehouse, human resources, security, and EH&S personnel Potentially senior executives (e.g., CEO and COO) and legal	No process-specific fraud controls Rely on entity-level ethics and compliance program, "speak-up" policy, and whistleblower program with anti-retaliation protection	Tested by IA — no findings	Medium — Collusion or management override of internal controls to conceal issues with major reputational or financial consequences, e.g., serious violation of emissions laws or regulations, or defective product safety features	Include follow-up questions in annual employee survey
NF3. Quality — employee certification test score tampering	Medium	Medium	Production, human resources, and security Potentially also sales management and sales personnel for affected customers and senior executives (e.g., CEO and COO)	No process-specific fraud controls Rely on entity-level ethics and compliance/fraud controls	Tested by IA — no findings	Medium — Collusion or management override of internal controls to tamper with test scores, e.g., to avoid violating provisions in a major contract	Revise testing procedure to require automatic recording and reporting of score results at test completion
NF4. Compliance — falsely reporting compliance information on contracts	Medium	Medium	Contract admin. unit, sales management, and sales personnel for affected customers Potentially senior executives (e.g., CEO and COO)	No process-specific fraud controls Rely on entity-level ethics and compliance/fraud controls	N/A	Medium — Collusion, bribes, kickbacks, or management override	Include follow-up questions in annual employee survey Will add a statement pertaining to company ethics and misconduct reporting to all purchase orders and contracts

For column explanations, please go to page 95.

Fraud Risk Assessment Example

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Section B. Non-financial Reporting							
NF5. Overstated/ false employee qualifications or certifications	Medium	Medium	All departments, especially sales management and sales personnel for affected customers Potentially human resources and senior executives (e.g., CEO and COO)	Confirmation of credentials via background checks on a sample of new hires whose qualification or credentials are to be relied upon for regulatory or contractual compliance or key organizational performance purposes	HR reports some findings — about 10% discrepancies	Medium — Involving personnel who lack required qualifications or credentials could violate provisions in customer contracts and introduce defects into the organization's products/ services, leading to financial claims against the organization, charges of false billing, disbarment as a government contractor, and reputational harm	Expand background testing to 100% Take swift, decisive action against people who have misrepresented their credentials Publicize internally (on a no-name basis) the disciplinary actions taken
NF6. Altered productivity reports	Low	Low	Production and operating unit management	Analytic comparisons of inventory consumption with labor hours	Monitored by IA — some fluctuations noted	Low - False reporting to earn productivity bonuses	None required due to low residual risk
Section C. Asset Misappropriation							
AM1. Cash theft by cyber fraud — professional fraudsters use phishing to obtain organization's online banking login credentials and severely deplete the bank accounts	Medium	High	Accounting and finance (including treasury)	Dedicated computer(s) for online banking use only — using other computers is strictly prohibited as is using this computer for any other purpose IT specialists set up the dedicated banking computer(s) with high security against both internal and external unauthorized access and use. Security measures are updated by IT security specialists on an ongoing basis All personnel with access to online banking credentials receive mandatory training about avoiding fraudsters' phishing techniques, using only the permitted computer(s) for online banking, and their responsibility to help ensure their colleagues comply very strictly with this policy, including the requirement to report any violations	Dedicated computer(s) are tested by IT security specialists to detect unauthorized or inappropriate use IA tests online banking transactions to the log of the dedicated computer(s) to identify transactions initiated elsewhere	Medium — emptying the organization's bank accounts would create a liquidity crisis that could severely disrupt operations	A separate team of IT security specialists will test the system security annually by trying to hack the system or obtain banking credentials through phishing, social engineering, "salting" thumb drives with malware, or posing as a cleaner or computer repair person Analytics to track trends in failed logon attempts, network access at unusual days/times, dates for last update of virus software, email with large attachments, etc.
AM2. Fraudulent disbursements — billing schemes — use of phony vendors	Medium	High	Contracting, purchasing, operations managers, or execs with significant procurement involvement (e.g., sales and marketing, IT, legal, general managers of remote locations, CEO or COO) Potentially accounting and finance	Purchases can only be made from approved vendors; vendors are approved by contracting department	IA tested — no findings	Medium — Employee could set up and get approved a phony vendor either through collusion or by fooling the contracts department, but it would be extremely difficult for this to be material to the organization	Establish a data analytic test that looks for any matching fields in the vendor and employee data-bases
AM3. Theft or diversion of inventory	Low	Medium	Warehouse, purchasing, security, general managers of business units, or site supervisors of remote locations	Physical access controls Comparison or purchase requisitions and receiving reports	IA reviewed and minor discrepancies noted	Medium — Collusion; concealment of purchases by delivery to off-site addresses	Begin using pre-numbered purchase requisitions that include statement that deliveries are only to be made to the warehouse address Implement data analytic tests comparing purchasing disbursements and inventory levels

For column explanations, please go to page 95.

Fraud Risk Assessment Example

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Section C. Asset Misappropriation							
AM4. Fraudulent disbursements — check tampering and expense reimbursement schemes	High	High if perpetrated by senior management or someone involved in financial reporting Low if perpetrated by other employees	Check tampering: accounting and finance (including treasury), contracting, purchasing, operations managers, or execs with significant procurement involvement (e.g., sales and marketing, IT, legal, general managers of remote locations, CEO or COO) Expense reimbursement schemes: all personnel but especially sales persons, sales management, and general managers of remote locations	Physical access controls, dual signatures on checks, support for expenses, review by supervisor and requirement that any false, statement on an expense report could be grounds for dismissal Awareness of pressures and incentives at all levels that may drive inappropriate financial behavior as well as observation, inquiry and other information that focus on lifestyle, family and personal financial issues of personnel in these departments	IA performs periodic review of disbursements at or near cutoff limits set for dual signatures or expense thresholds for receipts	Medium — if by senior management Low — if by other employees	Rotation of responsibilities in accounting and finance function, mandatory vacations, awareness of lifestyle and other personal issues such as divorce, illness, bankruptcies, and disgruntled employees who may want to get back at the organization
AM5. Cash skimming	Low	Low	Cashiers and cash room staff Potentially accounting and finance	Use of minimal cash transactions; cash reconciliations	Deemed effective	Low	None required due to low residual risk

For column explanations, please go to page 95.

Fraud Risk Assessment Example

1. Identified Fraud Risks and Schemes	2. Likelihood	3. Significance	4. Personnel/ Departments Involved	5. Existing Fraud Control Activities	6. Effectiveness of Existing Control Activities	7. Residual Fraud Risks	8. Fraud Risk Responses
Section D. Illegal Acts/Corruption							
IAC 1. Bribery of government officials	Medium — depending on type of contracts, permits, potential for influence by government official, etc.	High — could also depend on the location of the revenue source. Also, sales in foreign countries where the risk of corruption is high is another red flag	Sales and general managers of business units Potentially senior executives (CEO or COO), legal and accounting and finance	Strictly enforced policy against offering, giving, receiving, and soliciting anything of value to influence an official act by a public official, agent, or government employee Strictly enforced policy prohibiting bribing of foreign officials as well as making unauthorized facilitation payments to those individuals involved in customs, permitting the flow of goods, and other activities Examine contracts where U.S.-based government or foreign officials have had any involvement and determine the historical relationships between sales agents and sources of revenue to determine if there was inappropriate influence on the part of the government official by the sales agent Examine expense reports of sales representatives and promotional activities by country (foreign) managers	No discrepancies have been noted in the U.S.-based operations but concerns exist about sales in China, India, and South America	High — Sales personnel could become part of a corruption scheme (both wittingly and unwittingly) Huge fines and penalties, as well as criminal sanctions are realistic possibilities if the bribery schemes are not dealt with in a timely fashion	Data analytics on sales and expense transactions in high-risk locations to identify potentially suspicious transactions for further testing by IA Send quarterly statement about the organization's compliance and ethics program to all customers, vendors, sales agents, and independent contractors regarding their responsibility to report any violations of this program All employees will have annual ethics training and be required to affirm that they understand the compliance and ethics policies and sign off stating that they understand its provisions and they will comply with the program
IAC2. Conflicts of interest – undisclosed relationships or related party transactions that negatively impact an organization's reputation and may cause financial harm while benefiting the person with the relationship	High	High	Owners, directors, senior executives, managers of operating units, and general managers of remote locations Potentially purchasing, sales, legal, or any other department	Policy requires all employees, including senior management, to disclose any personal relationships, business transactions, and related parties in a timely manner for approval by the board or other governing body Background checks are performed on all key personnel, looking for undisclosed interests in businesses, real estate, or other relationships IA routinely uses data analysis tools to compare vendor and customer master files with employee payroll files, looking for matching addresses, names, tax identification or Social Security numbers, and telephone numbers	IA tested — no findings	Medium — Risk of management override of internal controls to conceal relationships and related party transactions	Use background check specialists to re-evaluate the organization's background check procedures and to test-check the results on selected individuals
IAC 3. Commercial bribery/illegal gratuities	Low	Medium	Sales, purchasing, general managers of business units Potentially senior executives (CEO or COO), legal and accounting and finance	Background checks on all purchasing personnel that look for bankruptcies, divorces, financial problems, criminal history Ensuring that all vendors are logged in, vetted, approved by a supervisor, and selected on a competitive bid basis IA performs routine audits of purchasing department	No discrepancies have been noted	Medium — Kickback schemes usually result in higher prices for goods purchased (reflective of the amount "kicked back")	Add a statement about the organization's compliance and ethics program directed at vendors requiring them to report all suspicious activities, solicitations, and misconduct relating to purchase orders and contracts

For column explanations, please go to page 95.

Fraud Risk Assessment Example

Column Explanations:

1. **Identified Fraud Risks and Schemes:** This column will include a robust list of the potential fraud risks and schemes that the organization may face. This list will be different for different organizations and should be informed by sources such as (a) industry research, (b) media reports, (c) interviews of employees and other stakeholders, (d) brainstorming sessions, and (e) activity reported through the whistleblower system and ethics program.
2. **Likelihood:** To design an efficient Fraud Risk Management Program, it is important to assess the likelihood of the identified fraud risks so that the organization can consider likelihood, as well as significance, in prioritizing its allocation of resources for fraud risk management. For purposes of the initial assessment, it is typically sufficient to evaluate the likelihood of risks as low, medium, or high. Following an initial assessment, use of a 1–10 scoring system can facilitate a more sophisticated ranking of risks, but this may be too complicated or unnecessary for some organizations.
3. **Significance:** Quantitative and qualitative factors are considered when assessing the potential significance of fraud risks to an organization. For example, certain fraud risks may only pose an immaterial direct financial risk to the organization, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the organization. For purposes of the initial assessment, it is typically sufficient to evaluate the significance of risks as low, medium, or high. Following an initial assessment, use of a 1–10 scoring system can facilitate a more sophisticated ranking of risks, but this may be too complicated and unnecessary for some organizations.
4. **Personnel/Departments Involved:** Identifying which people inside and outside the organization (by role/title, not by name) could be involved in perpetrating a particular fraud scheme will help to differentiate similar fraud schemes that may have considerably different likelihood or significance depending on who is involved, e.g., an individual salesperson reporting fictitious sales versus the CEO or CFO doing so.
5. **Existing Fraud Controls Activities:** Map pre-existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for their inherent likelihood and significance. By progressing in this order, this framework intends for the organization to assess identified fraud risks on an inherent basis, without consideration of internal controls.
6. **Effectiveness of Existing Control Activities:** Evaluate whether the identified fraud controls are designed and operating effectively to mitigate the specific fraud risk under consideration, taking into consideration who might be involved as perpetrators and their ability to override or circumvent certain controls.
7. **Residual Fraud Risks:** Consider the extent to which internal controls mitigate (reduce) each fraud risk and compare this to the board's fraud risk tolerance. Some fraud risks may not be mitigated adequately due to several factors, including (a) properly designed controls are not in place to address certain fraud risks or (b) controls identified are not operating effectively.
8. **Fraud Risk Responses:** Fraud risk responses are appropriate to address residual fraud risks that exceed the organization's risk tolerance as set by those charged with governance. Responses may include one or a combination of the following: (a) implementing additional controls, (b) designing proactive fraud detection techniques, (c) reducing the risk by changing the organization's processes, or (d) eliminating the risk by exiting the activities that generate the risk (e.g., avoiding intolerable corruption risks by ceasing to do business with countries X and Y).

APPENDIX F

Fraud Risk Management Tools

The following tools reside on the ACFE website. These will be updated and improved periodically. Suggestions for improving these tools or adding more tools will be welcomed. Email suggestions to FRMG@acfe.com.

Interactive Fraud Risk Management Scorecards — These scorecards facilitate an assessment of each of the five Fraud Risk Management Program components. The scorecards can be used to assess how well an organization has implemented the five fraud risk management principles to aid in determining how comprehensive an organization's Fraud Risk Management Program is, how well it is achieving its objectives, and where it needs to be improved. After each scorecard is completed, the tool generates a report that (a) summarizes how well the organization is adhering to each Point of Focus within that Principal and (b) displays which elements were scored as red (not yet implemented), yellow (partially implemented), and green (fully implemented).

Points of Focus Documentation Templates — These templates facilitate creation of consistent and uniform documentation of how the organization has implemented fraud risk governance, the fraud risk assessment, fraud control activities, fraud investigation and follow-up, and fraud risk management monitoring.

Risk Assessment and Follow-up Actions Template — This Excel spreadsheet facilitates performance and documentation of the fraud risk assessment. The user starts by documenting the fraud risk assessment using the assessment matrix format presented in this Guide. Once the risk assessment matrix has been completed, the spreadsheet:

- Automatically creates a heat map graphic displaying the significance and likelihood of each identified fraud exposure
- Automatically populates a Fraud Risk Ranking page that shows each fraud risk exposure from most to least severe and provides a space to record the organization's response plan for each exposure
- Automatically populates a Control Activities Matrix that facilitates the identification and evaluation of existing control activities related to each fraud risk exposure, and provides space to identify additional control activities for each exposure
- Contains a page to record allegations of suspected fraud, document investigations, and display outcomes
- Contains a page that facilitates documentation of fraud risk management monitoring plans, actions, deficiencies, and corrective actions

The tool also contains an example of a completed risk assessment matrix, heat map, Fraud Risk Ranking, and Control Activities Matrix

Anti-Fraud Policies and Procedures — These are sample materials that can be used to facilitate implementation of a comprehensive Fraud Risk Management Program. Included are the following:

- Sample Fraud Control Policy Framework — a listing of key elements to be considered in drafting a fraud control policy
- Fraud Risk Management High-Level Assessment — a checklist to use to make an initial high-level assessment fraud risk governance policies
- Sample Fraud Policy Responsibility Matrix — a sample tool that can be used to summarize and visualize the fraud risk governance roles and responsibilities that have been defined for an organization as part of its Fraud Risk Management Program
- Sample Fraud Risk Management Policy — a sample policy document that can be adapted to meet the needs of a particular organization
- Sample Fraud Risk Management Survey — a sample survey that can be modified as needed for a particular organization and administered periodically to assess organizational awareness regarding fraud risk management

Library of Anti-Fraud Data Analytics Tests — To assist organizations in getting started with integrating data analytics into their fraud risk assessment or investigative work plans, this library of test examples displays a variety of tests to consider related to many common fraud risk exposures. These tests are organized by asset misappropriation, corruption, and financial misstatement classification categories and are designed to provide general guidance and examples for consideration in forensic data analytics efforts.

Anti-Fraud Playbook — The Anti-Fraud Playbook provides best practices and tools for implementing, improving, and benchmarking an organization's Fraud Risk Management (FRM) Program. Designed to align with the *Fraud Risk Management Guide*, the 10 plays outlined provide easy-to-use, actionable guidance. The playbook also includes key questions, checklists, and insights that will enhance your FRM Program and ultimately facilitate proactive FRM at your organization.

Fraud Risk Exposures — This is a list of possible fraud schemes that can victimize an organization. The list contains fraud exposures that all organizations need to guard against and also schemes within different industries (healthcare fraud, financial services, manufacturing, and so forth). Each scheme listed is hyperlinked to an underlying description of the fraud and how it can be carried out. The exposures list can be used either (a) as a starting point for a fraud risk assessment (does our organization need to be concerned about this exposure?) or (b) as a final check once a fraud scheme list has been compiled by the risk assessment team. This list is intended to be expanded to cover new and emerging frauds. Suggestions for additions to this list will be welcomed. Email suggestions to FRMG@acfe.com.

APPENDIX G

Managing the Risk of Fraud, Waste, and Abuse in the Government Environment

Globally, governments face the common challenge of managing the risk of fraud, while carrying out missions that are highly complex and diverse. The legislative or regulatory design of some programs may open the door to fraud or otherwise increase fraud risk, such as not permitting verification of need for certain benefits. Compounding the challenge, waste and abuse in government programs may be viewed by the public through the same lens as fraud. Governmental stakeholders — citizens — expect government to safeguard all public funds and assets.

Despite some significant differences between governmental and non-governmental organizations, the essential elements of fraud risk management are the same and align with the COSO Framework and the concepts discussed in this COSO *Fraud Risk Management Guide* (COSO FRMG). This appendix discusses the government environment and presents a practical approach to successfully managing fraud risk in government.

The Government Fraud Risk Environment Markedly Differs from the Private Sector.

It is important to first understand the government fraud risk environment. It markedly differs from the private sector and, as well, can differ markedly between developed and emergent countries, and even among developed countries and levels of government. In countries where public corruption may be extensive and accountability and transparency virtually non existent, there are limits to what is possible to mitigate fraud risk without major cultural and legal changes that go far beyond the mechanics of instituting a Fraud Risk Management Program.

Governmental organizations carry out enterprise activities similar to non-governmental organizations. That includes payment and collection operations, procurement, personnel management, manufacturing, accounting, and finance. As a result, governmental organizations are vulnerable to all the same fraud risks that non-governmental organizations face. The nature of governmental organizations, programs, activities, and functions, however, adds a wide range, variety, and magnitude of additional fraud risks that non-governmental organizations do not face.

The United States (U.S.) is the focus of discussion in this appendix given its extensive network of government organizations and structures, but these concepts are applicable to governmental organizations worldwide. In the U.S., governments range from the huge federal government and its dozens of departments and hundreds of agencies (some of which are larger than some national governments) to large and small states to big cities and small towns to municipal school and water districts. It is certainly not one-size-fits-all in the U.S., but the same types of issues generally apply to the environment of other governments globally, especially in developed countries.

Fraudsters will go where there is money and opportunity, and government programs offer both.
Criminals follow the money, targeting large programs first and foremost. Any large government program is highly susceptible to fraud, because the opportunities and temptations to the criminal element are just so great. Government programs range from massive benefit, retirement, healthcare, and lending programs to national defense and homeland security to education and housing to disaster assistance.

There are thousands of government programs and operations, administered at all levels of government, by millions of government employees and active-duty military personnel, who are supported by millions of contractor staff. The federal government enters into multi-billion-dollar procurements, which are targets for fraud. Government steps in where no one else would or could, which presents enormous risk. Certain government programs may take on risks for the public good, such as flood insurance. Also, programs may be duplicative, overlapping, or redundant or can be largely administered by one level of government on behalf of another, all of which can foster a greater risk of fraud. Also, even relatively small local governments, where controls may be largely a matter of trust, experience significant cases of fraud. For example, the treasurer of the town of Dixon, Illinois embezzled more than $53 million over more than 20 years. The town's annual budget during the latter years of the fraud was less than $18 million.

In the U.S., spending at all levels of government as a percentage of the U.S. gross domestic product has averaged around 35% over the past 30 years. For example, included is $2 trillion[23] of pre-COVID-19 spending in 2019 on government healthcare programs, such as Medicare and Medicaid. While there are no exact numbers on fraud losses in government healthcare programs, estimates have ranged from 5% to 10%. There are concerted efforts by government agencies and law enforcement organizations to prevent and detect fraud against government healthcare programs and to prosecute offenders, but fraudsters remain persistent. For example, on September 17, 2021, the U.S. Justice Department charged 138 people with telemedicine and other healthcare fraud valued at $1.4 billion.

Fraud risk can take a back seat to public policy considerations, which are amplified in post-disaster environments.
The primary focus of most government agency leaders is program delivery, policy development and implementation, and not fraud risk management. Understandably, the risk of not meeting program goals and potential adverse impacts on public well-being, health, safety, and national security carry the highest priority in government. The bottom line is not profit and loss.

In addition, for some programs, fraud-related controls may be secondary to privacy considerations or the need to act quickly. There are programs where, by law, payments are triggered based on applying for benefits. For example, by design, legislation establishing the federal school lunch program did not permit school systems to require parents or guardians to provide supporting documentation proving need. The Congress recognized that some would fraudulently receive benefits that otherwise may not have been paid if there was some verification of need but viewed the potential negative impact on children as being more important. Disaster assistance programs are rife with fraud, waste, and abuse. When there is a natural disaster or what the world faced with COVID-19, governments immediately step in to help, quickly disbursing what can amount to tens of billions of dollars of assistance (or even trillions of dollars in the case of COVID-19). Addressing critical public needs is first and foremost to government. The door to benefits opens widely and quickly to meet urgent needs for assistance. These are situations that fraud perpetrators, from career criminals and citizens making false claims to contractors defrauding the programs, dream of, even when government is on the alert from the outset based on experience.

The fact that more could have been done at the front end of the application process for disaster assistance to prevent fraud is largely secondary to helping those in urgent need. Life and death relief cannot be denied because the victim of a disaster cannot produce eligibility documentation that was destroyed by the natural disaster itself. At the same time, government has learned the perils of not doing enough on the front end to at least deter the most egregious situations. The need to subsequently detect and chase collection of these misappropriated amounts is often unsuccessful as fraudsters are typically long gone.

In a crisis, governments must have speed and agility in how they respond and, if needed, bypass normal procurement practices to expeditiously obtain lifesaving goods and services. Around the world, governments will declare national emergencies and quickly activate emergency procurement regulations to accelerate their response by providing greater flexibility. For example, the Open Contracting Partnership estimated that by July 2020 at least $100 billion had been spent on COVID-19-related procurements. With that much being expended and at the speed it was being spent, the Partnership cited an increased risk of corruption and fraud.

Meeting the urgent needs presented by a national emergency and maintaining the necessary flexibility to do so, while also implementing effective integrity controls to detect and prevent corruption and fraud is challenging. Even when emergency declarations allow expedited spending, governments around the world still need to consider what is reasonable and justifiable given all the facts and circumstances at the given time. Governments must balance the need to act without delay (for example to save or preserve life) with meeting their overarching public-sector obligations to act lawfully, reasonably, and with integrity. Governments need to learn from the past in preparing for the future by developing the processes and systems needed in times of disaster so there is a clear game plan.

System shortfalls leave the door open to fraud.
Fraud is enabled many times by outdated information technology (IT) systems in many areas of federal, state, and local government. Many government agencies maintain antiquated IT systems that are not integrated, cannot scale to increased levels, and cannot share information across government entities. This was particularly evident during the COVID-19 pandemic. As a result, fraudsters can more easily obtain fraudulent benefits and do so from different government agencies at the same time.

For example, large-scale fraud was prevalent during the avalanche of applications for unemployment insurance (UI) as part of COVID-19 economic relief. Within the 17-week period ending July 11, 2020, some 51 million Americans applied for UI, representing more than a quarter of the U.S. workforce and 10 times the number of UI claims for all of 2019. Antiquated state IT systems, some dating to the 1970s, and existing claims processing staff could not manage the unprecedented volume in a timely manner. The sudden deluge of claimants was further exacerbated by the expansion of benefits to people normally ineligible for UI and the easing of certain eligibility requirements and normal internal controls, such as fully validating recipient eligibility before disbursing funds. One state auditor reported that the state stopped "approximately $12.8 billion in potentially fraudulent payments" but "also approved almost 597,000 claims totaling $10.4 billion in payments that might have been fraudulent." Included were more than 1,700 UI claims from the same address, and about $810 million in allowed claims filed under the names of prisoners.[24] Such blatant fraudulent claims could have been prevented or mitigated through the application of data analytic techniques discussed throughout this *Fraud Risk Management Guide*. Government organizations can and need to eliminate low-hanging fruit that is identified during every disaster.

With so many benefit programs, identity theft remains a huge risk for governments. In January 2021, the National Association of State Workforce Agencies and its UI Integrity Center reported that identity theft is the biggest challenge for states in addressing potential UI fraud. The information that criminals need to steal someone's identity is readily available on the Dark Web for a relatively nominal cost. This problem has been profoundly exacerbated by the large numbers of data breaches that have occurred over the last decade. The proliferation of personally identifiable information available for sale to fraudsters has created an identity theft epidemic which government agencies are only recently beginning to understand. During the pandemic, criminal takeovers of legitimate claimants' UI accounts to reroute benefits to other accounts increased dramatically. Also, the same fraudsters made claims in multiple states knowing that the state systems were not designed to share information and cross-check UI applicants.

[23] Congressional Research Service, "U.S. Health Care Coverage and Spending," Jan. 26, 2021.

[24] California State Auditor, "Employment Development Department: Significant Weaknesses in EDD's Approach to Fraud Prevention Have Led to Billions of Dollars in Improper Benefit Payments," Report 2020-628.2, Jan. 21, 2021.

Managing the Risk of Fraud, Waste, and Abuse in the Government Environment

The U.S. government does not stand alone in being victimized by fraudsters during COVID-19. Brazil's Office of the Comptroller General (CGU) identified over 680,000 public officials from federal, state, and municipal governments who received the equivalent of $181 million USD in emergency economic relief benefits. The payments to these public officials were potentially mistakenly paid and/or their personal information fraudulently used to request the aid.[25]

Cyberattacks have changed the fraud risk management game.
Cyberattacks from anywhere in the world plague governments and the private sector globally. Whether nation states, terrorists, or fraudsters, cybersecurity is a serious problem in U.S. government, with cyber warfare among the nation's highest national security risks. For example, in late 2020, a major supply chain attack (commonly known as SolarWinds), impacting government and private-sector companies in the U.S. and globally, was discovered. Cybersecurity experts expressed hope that this attack, termed one of the most serious in U.S. history, would accelerate the implementation of enhanced cybersecurity that focuses on a "zero trust" cybersecurity framework.[26] Also, there has been a pronounced growth in high-profile ransomware attacks that deny access to critical data and systems until a ransom is paid and in the introduction of spyware to eavesdrop on Americans.

From the U.S. Government Accountability Office (GAO) in its March 2021 "High-Risk Series" report: "Federal agencies and our nation's critical infrastructures…are dependent on IT systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is vital to public confidence and national security, prosperity, and well-being. …The risks to IT systems…are increasing, including insider threats from witting or unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and more destructive attacks. We have designated information security as a government-wide high-risk area since 1997."

The vast majority of government revenue comes from taxes, with significant tax evasion and tax fraud estimated to be 15%.
While the private sector has to worry about revenue collection for sales of goods and services, governments grapple with tax collections. The reported U.S. federal government tax gap — the difference between taxes collected and taxes owed — was estimated by the U.S. Department of the Treasury to be about $600 billion for 2020, or about 15%, with a 10-year estimate of $7 trillion.[27] The federal tax gap includes those who willfully violate tax laws and otherwise commit fraud, primarily through willful underreporting and identity theft. There are no easy answers to tax fraud, and the degree of oversight and tools used in enforcement are guided by law and public policy. Fraud risks increase when tax collection agencies are understaffed and lack modernized IT systems and operations. A private-sector company places collection of revenue as a top priority, which is not always the case in government.

The lines between fraud, waste, and abuse are often blurred, making it more difficult to have a clear picture of the magnitude and root causes of fraud.
Fraud, waste, and abuse need to be considered together and attacked no matter the cause of the risk. Sometimes the only difference may be in how a problem is legally addressed, such as when a company or individual settles with the government without admitting to any wrongdoing for what could arguably be considered fraud. Also, what initially appears to be "just" waste or abuse could ultimately turn out to be fraud. An example is the award of a contract for unneeded or overpriced goods and services, which would be considered wasteful on its face, but could also involve procurement fraud, such as bribery of government employees and public officials.

Improper payments, which have long been a high-risk area in the federal government, totaled a reported $277 billion for fiscal year 2021 alone. The U.S. Office of Management and Budget (OMB) defines improper payments as, "overpayments and underpayments, any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), any payment that does not account for credit for applicable discounts, and any payment for which an agency's review is unable to discern propriety due to insufficient documentation." Improper payments can fall into fraud, waste, or abuse depending on the root cause. Not all improper payments are fraud, but all improper payments are wasteful to the government.

According to GAO:

Fraud involves "obtaining something of value through willful misrepresentation."

Waste is "the act of using or expending resources carelessly, extravagantly, or to no purpose." Waste does not typically constitute abuse or necessarily involve a violation of law as is the case with fraud. Instead, it relates primarily to mismanagement, inappropriate actions, and inadequate oversight.

Abuse is a "behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances, but excludes fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements. Abuse also includes misuse of authority or position for personal financial interests or those of an immediate or close family member or business associate."

While reports of waste and abuse in government programs are more prevalent than fraud, the public may not differentiate between the three and usually does not care about how or why money is misspent. The fact that money was misspent is the problem. These situations undermine public confidence, because government is expected to collect and safeguard every tax dollar and every asset. In addition, in government, even the most immaterial fraud, waste, or abuse by a government official or employee can be serious in the eyes of the public. Especially when a high-level official is involved, it may be in the news for weeks or months and the subject of Congressional hearings. Conversely, a major fraud against the government can quickly become old news and may largely be viewed by the public as a failure by government to safeguard tax dollars.

Government has a very strong independent audit and investigation capability.
Independent, non-partisan audit and investigation organizations are a key component of fraud risk management in government. An army of government auditors focus not only on fraud, waste, and abuse but on program delivery and mission effectiveness. Their work goes far beyond traditional internal audit and financial statement audits in the private sector, and the results of this work are transparent to the public.

GAO, which serves as the Congressional "watchdog," has over 3,200 staff, including a Forensic Audits and Investigative Services team. GAO is led by the Comptroller General of the United States, who is Presidentially-appointed and Senate-confirmed, with a 15-year term, providing unparalleled independence. The Comptroller General can only be removed through impeachment, and this has never happened in GAO's 100-year history during which only eight individuals have served in this important oversight role.

Recognizing the seriousness of government fraud, waste and abuse, Congress enacted the Inspector General Act of 1978 (Public Law 95-452, October 12, 1978), that has since been amended several times, to establish independent auditors and criminal investigators in major federal agencies. IGs are dual-hatted, meaning they provide the same type of information to their agency management and Congress, while still not being directly supervised by either. They provide audit findings and recommendations internally to agency management as fully independent auditors and investigators, with broad powers (including subpoena and other law enforcement authorities) far beyond an internal auditor in the private sector. They also report externally to Congress and the public making them effective "watchdogs" of the government. IG reports are publicly available on their websites, and IGs also prepare semi-annual reports that summarize their findings and impact. Because of their independence from agency management, under *Government Auditing Standards*, which are promulgated by the Comptroller General, IGs are considered independent external auditors.

There are over 70 statutory federal agency-level inspectors general (IG) — over 30 of which are Presidentially-appointed and Senate-confirmed. These IGs provide oversight for about 99% of federal funds. There are also Special IGs, such as for Pandemic Recovery spending and for Troubled Asset Relief spending. In addition to statutory IGs, there are other federal agency IGs that are created by regulation within their individual federal agency. There are also various state, county, and city IGs that oversee state, local, and federally provided funds. Lastly, there are 50 state auditors, with about half elected officials, supported by thousands of auditors and investigators, and there are thousands of city and county auditors similarly charged with attacking fraud, waste, and abuse on behalf of the public.

U.S. government IG and audit organizations will often primarily conduct performance audits and administrative and criminal investigations, such as reviews of program performance and internal controls and investigations into potential wrongdoing. In the federal government, audits of agency financial statements are primarily performed by independent public accounting firms, often under contract to and subject to oversight by a federal IG or a state, city, or county auditor. Government audit and investigative reports (except criminal investigations) are generally available to the public, typically on readily accessible websites. This provides public transparency far beyond a private-sector company. Finally, there is a network of fraud hotlines and extensive whistleblower protections at all levels of government, generally mandated by various laws or regulations, that are a critical tool for government oversight bodies to learn of areas of fraud, waste, and abuse.

In addition, the federal government establishes strong, real-time oversight and reporting for certain high-risk, emergency spending programs rather than just assessing what agencies have done after the fact. The American Recovery and Reinvestment Act (ARRA) of 2009 (Public Law 111-5, February 14, 2009) was landmark legislation, not only because of the economic impact of stimulus funding to address the 2008 financial crisis, but due to greatly increased transparency, standardized public reporting of obligation and disbursement activity, and continuous oversight. The Recovery.gov web site gave the public unprecedented, near real-time visibility into the distribution and use of stimulus funds. In effect, the public provided another set of "oversight eyes."

The IGs had an unprecedented oversight role through the ARRA Recovery Accountability and Transparency Board (Recovery Board). IGs were on point to proactively monitor spending and immediately identify and investigate potential problems. The Recovery Board used powerful analytic tools and leveraged complimentary skills of highly trained auditors, investigators, and data analysts. There were partnerships at all levels of government since certain ARRA funding was administered directly by states and localities. As well, the government audit community — federal IGs, state and local IGs and auditors, and GAO — closely coordinated their efforts. The former ARRA Recovery Board chair was quoted as commenting that "Historically, fraud losses on big government outlays usually run between 5% and 7%. … Recovery (Board) kept the losses at less than 1% with a very sophisticated enterprise."[28]

[25] gov.br/cgu/pt-br/assuntos/noticias/2020/08/cgu-identifica-agentes-publicos-que-receberam-auxilio-emergencial-de-forma-indevida.

[26] Tony Hubbard, Joseph Klimavicz, Steve Wong, and Jeffrey Steinhoff, "Zero Trust in a Virtual Cybersecurity World," Association of Government Accountants (AGA) *Journal of Government Financial Management*, Summer 2021.

[27] Natasha Sarin, "The Case for a Robust Attack on the Tax Gap," Deputy Assistant Secretary for Economic Policy, U.S. Department of the Treasury, Sep. 7, 2021.

[28] Adam Zagorin, "He Oversaw $787 Billion in Stimulus Spending; Here Are His Lessons on Spending Coronavirus Recovery Effectively," Project on Government Oversight, April 1, 2020.

Managing the Risk of Fraud, Waste, and Abuse in the Government Environment

Applying these lessons learned has provided a road map for oversight of COVID-19 relief spending, totaling an unprecedented $4.6 trillion, almost six times the $800 million spent on ARRA. The Coronavirus Aid, Relief, and Economic Security (CARES) Act of 2020 (P.L. 116-136, March 27, 2020) created the Pandemic Response Accountability Committee (PRAC), patterned after ARRA's Recovery Board. Composed of IGs, the PRAC is charged with (1) "preventing and detecting fraud, waste, abuse, and mismanagement" by independently reviewing and reporting on the federal government's response to the coronavirus pandemic and use of funds and (2) finding out "where pandemic response program dollars are being spent" through interactive data visualizations and maps. The CARES Act also created the Special IG for Pandemic Recovery, responsible for oversight of $500 billion of relief to large corporations deemed critical to national security, such as air carriers.

This governmental focus on COVID-19 fraud has been critical, especially since new programs were rapidly established — some with dramatically greater funding than existing programs. For example, pre-COVID-19 funds available to the Small Business Administration (SBA) for fiscal year 2020 totaled almost $1.2 billion. Administered by SBA, funds for the new COVID-19 Paycheck Protection Program (PPP) totaled almost $800 billion over 14 months. PPP loans, which are eligible for forgiveness, are highly vulnerable to fraud, waste, and abuse.[29]

On June 25, 2020, GAO reported: "Because of the number of loans approved, the speed with which they were processed, and the limited safeguards, there is a significant risk that some fraudulent or inflated applications were approved. In addition, the lack of clear guidance has increased the likelihood that borrowers may misuse loan proceeds or be surprised they do not qualify for full loan forgiveness." GAO recommended that SBA develop and implement plans to identify and respond to PPP risks to better ensure program integrity. Subsequently, extensive fraud has been identified in PPP spending and criminal charges for fraud continue to be made.

The movement to "open government" public reporting provides a window to fraud, waste, and abuse not available in the private sector, but data quality and advanced analytic tools remain a challenge.

While it varies greatly by country, in the U.S., reports of fraud, waste, and abuse are largely open and transparent to citizens and not limited to top management, boards of directors, or audit committees. Citizen visibility and awareness can drive action to address fraud risks. Globally, international organizations, such as Transparency International, Open Contracting Partnership, and Open Ownership, continue to promote access to government information and transparency on the use of public funds. In some countries, government funds are provided to create and operate civilian society watch-dog organizations to help identify potential fraud, waste, and abuse of public funds.

As highlighted earlier, all spending related to ARRA was reported on a publicly accessible website, as is spending to fight COVID-19 and provide financial relief. The public has been given access to the information and the tools to drill down several layers into the data. There have been millions of public hits on these websites, and citizens are viewed as extra sets of eyes auditing the information. With only a few exceptions, this has now been expanded to all federal government spending. You do not see this expansive, open reporting and transparency in the private sector or in most other governments.

At the same, the quality of government data critical to fighting fraud can be problematic. Legislation, such as the Data Accountability and Transparency Act (DATA Act) of 2014 (Public Law 113-101, May 9, 2014) and the Foundations for Evidence-Based Policymaking Act (Evidence Act) of 2018 (Public Law 115-435, January 14, 2019), continue to expand online reporting and focus on data quality. The DATA Act raised the information bar by requiring government-wide data standards and increased data availability (such as through public reporting on USASpending.gov), accuracy, and usefulness. A sound data standardization framework is critical to users' ability to analyze and understand spending data; reach meaningful conclusions about value and performance; and attack fraud, waste, and abuse. The Evidence Act mandates "systematic rethinking of government data management to better facilitate access for evidence-building activities and public consumption."

The quality and completeness of open government data remain a work in process, with needed additional focus on data collection, data sharing, and data analytics. As discussed earlier, antiquated IT systems that are not integrated impair the ability to enhance data quality. The challenge is to take the massive amount of data that governments maintain and turn it into actionable information for decision-making and oversight through ever-more powerful analytic tools.

The COSO and Federal Internal Control Fraud Risk Frameworks Align, But Implementation of Certain Concepts May Differ.

While the government fraud risk environment understandably differs from the private sector, the COSO 2013 *Internal Control — Integrated Framework* and the concepts in this FRMG, which follow COSO, equally apply to government and the private sector. There may be some areas where the government is different, such as the establishment of independent IGs, open government public reporting, and law enforcement authorities, but the primary control objectives align.

To varying degrees, governments in the U.S. have adopted the COSO 2013 IC Framework or apply similar concepts. The word "varying" is important because governments are so diverse in size and mission, ranging from the federal government with about four million civilian and military personnel to a local township with just a handful of employees. Also, where the framework has been adopted, implementation of certain concepts may be different.

Because there is no one model in the U.S. government, in discussing the alignment between the COSO 2013 IC Framework and internal control frameworks adopted by governments in the U.S., the federal government is being used as a case study. The federal government first adopted an internal framework similar to COSO's *Internal Control — Integrated Framework* in 1982, and subsequently embedded the COSO 2013 IC Framework in its internal control standards.

Federal laws and regulations foster strong risk management consistent with the COSO framework.

The federal government's approach to fraud risk management is supported by legislation and implementing standards, regulations, and guidance mandating leading practices. A strong legislative standing is an important means of fostering attention at the highest levels in governmental organizations on fraud risk management.

Expectations for addressing fraud, waste, and abuse took a significant step forward in 1982 with enactment of the Federal Managers' Financial Integrity Act (Public Law 97-255, September 8, 1982). At the heart of the act is management control, which goes far beyond financial reporting to the controls used to manage programs and operations; thereby dovetailing with the concepts in the COSO 2013 IC Framework. The Financial Integrity Act reinforced management's responsibility for internal controls by requiring federal agencies to perform annual self-assessments of their internal controls and accounting practices and to publicly report the results in an agency head assurance statement to the President and the Congress. For example, in the Department of Defense, the assurance statement is signed by the Secretary of Defense and component assurance statements are signed by the military department heads, such as the Secretaries of the Army, Navy, and Air Force.

The Financial Integrity Act required the U.S. Comptroller General to issue internal control standards and the OMB to issue implementing guidelines to be used in assessing and reporting on internal controls. These standards and implementing guidelines are essential components of fraud risk management. The COSO 2013 IC Framework is embedded in the *Comptroller General's Standards for Internal Control in the Federal Government* (commonly called the "Green Book"). The Green Book standards (further discussed below) apply equally to program and mission implementation and administrative and financial operations and are intended to help both program and financial managers.

In turn, these standards undergird OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, which was updated in July 2016. In defining management's responsibility, Circular A-123 emphasizes "the need to integrate and coordinate risk management and internal control into existing business activities and as an integral part of managing an Agency." The July 2016 circular, among other things, specifically addresses enterprise risk management (ERM) and managing program fraud risks, including a requirement to evaluate fraud risks and to use a risk-based approach to design and implement financial and administrative activities to mitigate identified material fraud risks. There is specific discussion on managing fraud risk in disaster situations, which has long been a vexing problem, as highlighted earlier. Circular A-123 also includes an illustrative example of a fraud risk profile, as well as illustrative risk profiles in other areas, such as grants management.

Supporting tools designed to help federal agencies meet the requirements of OMB Circular A-123 are included in the *Playbook: Enterprise Risk Management for the U.S. Federal Government* (ERM Playbook), issued by the Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC) on July 29, 2016.

GAO's Green Book is designed to be broadly used by all three levels of government in the U.S.

A leading practice for governments is to either develop their own internal control standards or adopt internal control standards of other organizations that are deemed applicable. The GAO Green Book standards were designed to be broadly used in government internal control and Fraud Risk Management Programs at all levels of government in the U.S. — federal, state, and local.

First issued in 1983 and established expressly for the federal government pursuant to the legislative mandate in the Financial Integrity Act, the Green Book was updated in 1999, in part to adapt to COSO's 1992 Integrated Framework. The Green Book was most recently updated in September 2014 to adapt to the COSO 2013 IC Framework for a government environment. The Comptroller General recognized the potential usefulness of the Green Book standards to other governmental entities. The forward of the 2014 Green Book, states:

> *The Green Book may also be adopted by state, local, and quasi-governmental entities, as well as not-for-profit organizations, as a framework for an internal control system. Management of an entity determines, based on applicable laws and regulations, how to appropriately adapt the standards presented in the Green Book as a framework for the entity.*

As highlighted earlier, the Green Book defines fraud as "willful misrepresentation to obtain something of value." In government, fraud represents an obstacle to an entity's ability to achieve its objectives and build trust. Mitigating the risk of fraud is based, in large part, on the significance of the fraud risk and the controls an entity has put in place as part of its internal control system. Principle 8 of the Green Book requires management to consider the potential for fraud as part of an effective internal control system. Specifically, the standards require management to consider the potential for fraud when identifying, analyzing, and responding to risks.

Government entities have an opportunity in managing fraud to take a strategic, risk-based approach to identifying and responding to fraud risks, including those risks that are non-financial in nature, such as reputational risk. The Green Book recognizes that implementing a risk-based approach to address potential fraud poses a unique set of challenges to governmental entities. As highlighted earlier, given their mission to provide the public with a broad range of critical, often time-sensitive services and financial assistance, government managers may perceive a conflict between their priorities to fulfill the entity's mission and taking actions to safeguard taxpayer dollars from fraud.

[29] Andrew Lewis, Nikki Reid, and Jeffrey Steinhoff, "Supporting the Nation's War Against COVID-19 Through Accountability, Transparency and Oversight," AGA *Journal*, Fall 2020.

Managing the Risk of Fraud, Waste, and Abuse in the Government Environment

Moreover, calculating the benefits of fraud prevention is challenging, given the difficulties in measuring the cost of fraud that does not occur as a result of fraud risk management initiatives. Government entities may be reluctant to pursue fraud risk management efforts if such efforts are perceived as hindering their primary mission. For instance, a preventive fraud control may reduce improper payments, but at the same time cause delays in payments or services to legitimate beneficiaries. However, the purpose of proactively managing fraud risks is to facilitate, not hinder, a government entity's mission and strategic goals by ensuring that taxpayer dollars and government services serve their intended purposes.

The key is to develop a Fraud Risk Management Program that effectively and efficiently finds the appropriate balance between program delivery and mitigating fraud risk to a reasonable level. As stated in OMB Circular A-123:

> *Federal managers must carefully consider the appropriate balance between risk, controls, costs, and benefits in their mission support operations. Too many controls can result in inefficiencies, while too few controls may increase risk to an unacceptable level.*

Across government, fraud can take many forms, and as highlighted earlier, some entities and programs are inherently more vulnerable to fraud than others. Likewise, expertise in combating fraud varies from entity to entity. Effectively managing fraud risks involves continuously mitigating the likelihood of fraud and its negative impacts on achieving an entity's mission.

As discussed in the Green Book, the objectives of an effective Fraud Risk Management Program are to prevent, detect, and respond to fraud, using a risk-based approach, with an emphasis on prevention. Similar to private-sector organizations, a risk-based approach in government recognizes that it is not possible to prevent all fraud from occurring and that, in general, the cost of preventing fraud should not exceed the cost the entity incurs from the fraud. Included in fraud prevention under the Green Book are:

- Building fraud risk management into government program design
- An organizational culture conducive to fraud risk management
- Execution of fraud risk assessments to identify and prioritize fraud risks
- Fraud awareness training
- Specific anti-fraud controls

From the Green Book, examples of *fraud prevention* controls, which are in line with COSO and private-sector organizations, are (1) up-front analytic tools to detect potential fraudulent or ineligible applicants for government programs and fraudulent or unsupported contract payments before funds are disbursed; (2) strong audit and investigative capabilities; (3) pre-established account limits; and (4) use of approved vendor lists.

Controls designed to *detect fraud* include data mining and data analytics, document reviews and data-base checks, fraud hotlines, whistleblower protection policies, and investigations. While detection is important, it should rarely, if ever, be the first line of defense. In the government environment, it is common for fraudsters to exploit vulnerabilities and quickly vanish. If they are caught, the assets are often gone. This represents a fundamental dilemma if program managers do not consider fraud risk at the outset and simply push money out the door to meet a public need and then later assess where the funds went. Leading government organizations ensure that fraud is always part of the equation and is continually re-evaluated and recalibrated to address current, changing, and emergent fraud risks.

Again, in line with COSO and the private sector, in the Green Book, fraud response is management's responsibility. In leading government organizations, this is clearly the case. However, some government organizations may view monitoring of effectiveness as a role of their IG or auditor general, internal auditor (where the legislative body has not established a legislative or appointed position), or the external auditor. An essential element of an effective Fraud Risk Management Program is management's day-to-day monitoring and evaluation to ensure that control activities are operating as intended and that timely action is taken to remediate any identified breakdowns and weaknesses. Management should always have its finger on the pulse of control breakdowns and fraud risks.

While the respective audit and investigatory organizations can play important roles in assessing fraud risk controls in operation, detecting, and investigating fraud and making recommendations to management on corrective actions to address identified fraud risks, the Green Book makes clear that management and staff of the organization must be actively engaged as the first line of defense. They must continually assess what can be a changing fraud risk environment and respond to fraud risks, including active monitoring and oversight and assurance that any auditor findings and recommendations for corrective actions are effectively and timely addressed.

The three objectives — prevention, detection, and response — are interdependent. For example, preventive efforts are generally more cost effective as they reduce the need for detective action. Response needs to address root causes of fraud risks and support stronger preventive and detective controls. This is no different than in the private sector. Government wants to avoid a pay-and-chase mode, which is far more costly and less effective than front-end prevention. Once fraud risks are identified, it is a matter of management's judgment to determine the significance of the identified fraud risks to its operations and determine what suite of activities and controls to put in place to mitigate those risks to an acceptable level.

Fraud risk management occurs throughout all components of an effective internal control system. As part of its control environment, a government entity considers how fraud risk could impact the organizational structure and designs the structure appropriately to reduce the risk of fraud occurring. If the significance of fraud risk to the entity's objectives is high, the entity may also consider identifying an anti-fraud unit or entity to manage this risk.

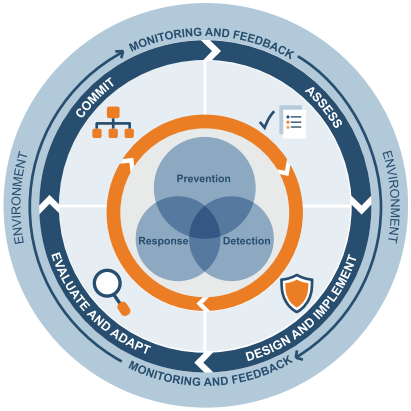
As stated earlier, in government, fraud risk goes far beyond monetary losses. Qualitative factors that impact the mission and program delivery, national security, or public health and safety can be the most important considerations in the government environment. For example, while both of the following scenarios represent problems government would like to avoid, fraud involving the sale of defective or substandard military equipment used by soldiers in combat would be a far more serious concern than if the government was fraudulently overbilled for combat equipment that met all military standards.

As discussed in the Green Book, a government entity designs control activities based on the actions management selected during the fraud risk assessment process. Management also considers whether entity-level controls may be a more appropriate response to fraud risk if the significance of the risk to the entity's objectives is not high.

In designing information and communication, a government entity may consider what information it would need to properly evaluate the risk of fraud, from both internal and external sources. Finally, as part of effectively monitoring the internal control system, a leading practice is to adopt both continuous monitoring activities and separate evaluations to assess the effectiveness of its actions, how well the entity is achieving its objectives, and how much impact, if any, control breakdowns and fraud are having on achieving those objectives.

GAO's Fraud Risk Framework, which has been adopted by OMB and supported by legislation, closely aligns to COSO's FRMG.

Complementing the Green Book, GAO developed *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework). OMB Circular A-123 requires that managers adhere to the Fraud Risk Framework's leading practices. GAO's Fraud Risk Framework organizes leading practices encompassing control activities to prevent, detect, and respond to government fraud, with an emphasis on prevention. It discusses structures and environmental factors that influence or help managers achieve their objective to mitigate fraud risks in federal programs. The Fraud Risk Framework also highlights the importance of monitoring and incorporating feedback, which are ongoing practices that apply to all four of the components described below in the following graphic.



Source: *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), GAO-15-593SP, U.S. Government Accountability Office, 2015.

As this graphic illustrates, the elements in GAO's Fraud Risk Framework require not only a strong management commitment, but also rigor in executing the elements of fraud risk management. The four components are no different than what private-sector organizations would implement and are closely aligned to the five components in the COSO FRMG.

Here is a crosswalk between the GAO Fraud Risk Framework components and the FRMG principles.

GAO Framework Component	*Fraud Risk Management Guide* Principle
1. Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.	**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.
2. Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.	**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.
3. Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.	**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.
4. Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management.	**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.

Managing the Risk of Fraud, Waste, and Abuse in the Government Environment

The one exception is that investigations, which is the fourth of five FRMG Principles, is not a component in the GAO Framework since federal agencies refer investigation activities to their inspectors general. If other levels of government in the U.S. or other countries use the GAO Fraud Risk Framework, they may need to consider investigations as an integral part of fraud risk management, depending on how they are structured.

Finally, the GAO Fraud Risk Framework includes valuable insights in a series of appendices covering:

- Challenges related to measuring fraud
- Examples of control activities and additional information on leading practices for data analytics and fraud-awareness initiatives
- Risk factors for assessing improper-payment risk
- Example of a fraud risk profile

Having a legislative mandate places additional emphasis on the importance of fully managing fraud risks. On June 30, 2016, the Fraud Reduction and Data Analytics Act (FRDAA) of 2015 (Public Law 114-186) was enacted. This federal law required OMB to issue guidelines for federal agencies to establish financial and administrative controls to identify and assess fraud risks and design and implement control activities to prevent, detect, and respond to fraud, including improper payments. FRDAA mandated that the OMB guidelines incorporate the leading practices identified in GAO's Fraud Risk Framework. OMB's revisions to Circular A-123, dated July 15, 2016, specifically require that federal agencies adhere to the GAO Framework.

Broader than just fraud, there have been legislative requirements, beginning with the Improper Payments Information Act of 2002 (Public Law 107-300, 116 Stat. 2350, November 2002) to measure and publicly report annually on all improper payments associated with federal funds, including amounts administered by state and local governments and grantees. The goal is improved payment performance through greater accountability and transparency.

FRDAA was repealed on March 2, 2020, with the enactment of the Program Integrity and Information Act (PIIA) of 2019 (Public Law 116-117), which also updated and replaced all existing improper payment legislation. With respect to fraud, PIIA provides that the OMB guidelines required to be established under FRDAA remain in effect, while providing that the guidelines can be periodically modified by OMB in consultation with the Comptroller General, as the OMB Director and Comptroller General may determine necessary. PIIA also specifies that the guidelines include (1) using a risk-based approach to design and implement financial and administrative control activities to mitigate identified fraud risks; (2) collecting and analyzing data from reporting mechanisms on detected fraud to monitor fraud trends and using that data and information to continuously improve fraud prevention controls; and (3) using the results of monitoring, evaluation, audits, and investigations to improve fraud prevention, detection, and response.

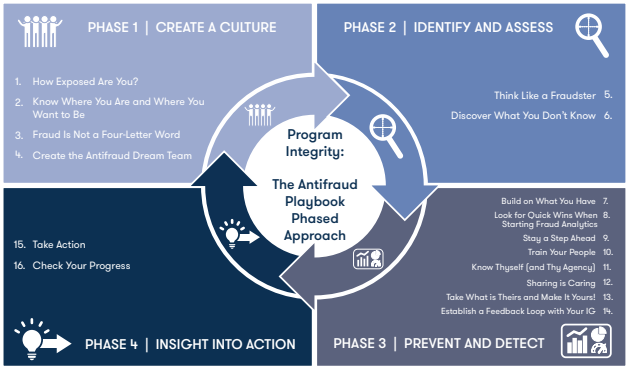
As part of its continuing fraud risk management leadership in the federal government, in January 2022, GAO launched its Anti-fraud Resource website, "Understand and Combat Federal Fraud." GAO's *Conceptual Fraud Model* is the primary source of the new website's content. GAO's model promotes a common understanding of fraud that affects the federal government. The model systematically organizes the key characteristics commonly found in fraud schemes affecting the federal government. Included are federal programs or operations that were affected by fraud schemes reviewed by GAO and all types of fraud scheme participants, activities, mechanisms, and impacts involved in those fraud schemes. Further, the model uniquely demonstrates the full complexity of fraud relationships that affect the federal government, such as how fraudsters use mechanisms to execute fraud activities. The web site highlights certain parts of the model to illustrate concepts in interactive graphics. The model can also be used to enhance data analytics by providing a common framework and vocabulary to describe and classify fraud that affects the federal government. To support wide user access, the model was developed using Protégé, which is a free, open-source software. WebProtégé, the online version of this software, provides a graphic user interface that can be used to review the complete model. (See gaoinnovations.gov/anti-fraud_resource/howfraudworks).

In addition, in October 2018, the federal CFO Council, in conjunction with the Department of the Treasury, issued the *Program Integrity: Anti-fraud Playbook* (Anti-fraud Playbook) for use by federal agencies and state and local government. The 102-page Anti-fraud Playbook is a tool to help enhance anti-fraud programs that support the fraud risk guidelines in OMB Circular A-123. As the opening of the Playbook states:

> *You can invest years in building your agency's reputation and public trust in it, and one incident of fraud can destroy it. The American people expect agencies to protect their tax dollars by developing and maintaining governance structures, controls, and processes to safeguard resources and assets. By making the management of fraud risk a priority at your agency, you can balance the achievement of your agency's mission with enhanced program integrity.*
>
> *How much does your agency lose annually in fraud? It is probably significantly higher than you think. The deceptive nature of fraud makes it extremely difficult to quantify because it is invisible until you discover it.*
>
> *This playbook provides a four-phased approach with 16 plays drawn from successful practices from the federal government and private sector to help you combat the risk of fraud at your agency. Combating government fraud is an ongoing challenge, but this playbook will provide you with practical and actionable guidance to help you in your anti-fraud journey.*

The Anti-fraud Playbook provides valuable insights that are useful not only to governments in the U.S., but globally. As shown in the following figure from the Playbook, the four phases are:

1. ***Create a culture*** conducive to both integrity efforts and furthering anti-fraud measures.
2. ***Identify and assess*** fraud risks and ***develop*** a path forward to execute, repeat, and expand fraud risk assessments that are unique and customizable to your organization.
3. ***Prevent and detect*** fraud through strong anti-fraud controls that mitigate your highest risks and fraud data analytics programs.
4. ***Turn insight into action*** by using available information to establish actionable tasks.



Source: *Program Integrity: The Anti-fraud Playbook,* Chief Financial Officers Council and U.S. Department of the Treasury, Bureau of Fiscal Service, 2018.

Enterprise risk management is critical to government fraud risk management.
Enterprise risk management (ERM) is an essential component of fraud risk management, whether in government or the private sector. COSO issued its *Enterprise Risk Management — Integrated Framework* (COSO ERM Framework) in 2004. COSO's premise, which is fully applicable in the government environment and consistent with the ERM requirements in OMB Circular A-123, is that "value is maximized when management sets strategy and objectives to strike a balance between growth and return goals and related risks, and efficiently and effectively deploys resources in pursuit of the entity's objectives."

COSO's bottom line in 2004 was that ERM "helps any entity get to where it wants to go and avoid pitfalls and surprises along the way." In 2017, COSO updated its ERM Framework. Now titled Enterprise Risk Management — Integrating with Strategy and Performance, the update "highlights the importance of considering risk in both the strategy-setting process and in driving performance." COSO identified 20 principles organized into five interrelated components: (1) governance and culture; (2) strategy and objective setting; (3) performance; (4) review and revision; and (5) information, communication, and reporting.

Similarly applicable to government and a cornerstone of OMB Circular A-123, there is a broad recognition in the federal government of the importance of considering internal control risk in the context of the enterprise. Controls are the policies and procedures established to achieve organizational objectives and to avoid what an organization does not want to happen. On the other hand, risks, such as fraud risks, are what can impair an organization's ability to meet its objectives. With an organization-wide view of risk, government agencies can be better positioned to quickly gauge which risks are directly aligned to strategic objectives, and which have the highest probability of impacting missions.

There can be a tendency, especially in large governmental organizations, to consider internal controls and fraud risks independently of each other. A key to success is to look across the enterprise and across stakeholders and business partners to better connect the dots. This improves management's understanding of control risks, while supporting fraud risk management, because fraud perpetrators look for disconnects. ERM helps government entities determine root causes that lead to breakdowns in control that foster fraud, waste, and abuse.

Fraud risk management is one component, albeit an important one, in taking an enterprise view in government. It is not just within a government entity that considerations of controls need to be integrated with fraud risks, but across levels of government and other stakeholders. For example, when one level of government provides funds to another level of government to carry out a program, it needs to understand the internal control and fraud risk environment at the recipient government entity as well as at other significant stakeholders, such as contractors, academic institutions, and not-for-profit recipients that may receive and administer government funds downstream.

Applying ERM concepts in government helps focus on the most important activities and corresponding controls by correlating the objectives to be attained and the amount of risk and/or cost government is willing to accept in return for defined results. COSO speaks about "aligning risk appetite and strategy." Cost-benefit is viewed from an enterprise perspective since risk appetite can vary between organizations within an agency. Risk appetite (discussed in greater detail below) provides the cornerstone for an agency ERM program.

Managing the Risk of Fraud, Waste, and Abuse in the Government Environment

Fraud risk considerations begin with establishing the risk appetite and are governed by policies that articulate the goals and objectives, roles and responsibilities, and strategies and tactics of implementation specific to fraud risk. Properly structured, both fraud risk management and ERM, are integral parts of all organizational processes and daily decision-making. Also, both explicitly address uncertainty and must be systematic, structured, timely, dynamic, iterative, forward looking, and responsive to change. As discussed earlier, the basic ERM and fraud risk framework and building blocks in government are no different than in the private sector.

ERM has gained significant traction in the U.S. federal government with formal recognition of the value of ERM as a management priority and revisions to OMB Circular A-123 expressly requiring agencies to adopt ERM. Based on the United Kingdom's *The Orange Book, Management of Risk – Principles and Concepts*, the management of risk at strategic, program, and operational levels at U.S. federal agencies are required by OMB Circular A-123 to be integrated so that the levels of activity support each other.

Some federal agencies have appointed chief risk officers (CRO) who champion risk management and advise senior leaders on the strategically aligned portfolio view of risks at the agency. The responsibilities of managing risk, however, are not solely the job of the CRO, but must be shared throughout the agency and owned by everyone — from the highest levels of executive leadership to the service delivery staff executing programs every day. To quote OMB,[30] an effective government CRO:

- "Develops, manages, coordinates and oversees a comprehensive system for proactively identifying, prioritizing, monitoring and communicating an organization's enterprise-wide risks. Such risks include relevant strategic, operational, financial, and programmatic barriers as well as reputational risks that could impede or interfere with an organization's defined strategic objectives and performance goals.
- Oversees the development and use of a robust set of risk management indicators that are representative of organizational operations and prioritized risks.
- Establishes and provides oversight of policies that enable consistent use of ERM principles and supports an integrated view of risk across the organization.
- Ensures the incorporation and dissemination of standard enterprise-wide risk management protocols and best practices to reduce duplication of effort and improve agency performance.
- Establishes the procedures for determining the amount of risk an agency will accept or mitigate, including the manner in which these elements of the decision-making process are documented.
- Creates and maintains institutional capacity and accountability for risk management through the exchange of information, knowledge, education, and training staff. All these duties apply in the context of fraud risk management, which should be an integral part of the CRO's job. Implementing Fraud Risk Management Programs, in tandem with ERM concepts, represents not only significant operational change in many governments but also, and perhaps more importantly, cultural transformation.

Further, OMB Circular A-123 specifies that leading government Fraud Risk Management Programs:

- Identify and break down barriers that can stand in the way of addressing fraud risk across the organization, with special focus on eliminating disjointed structures and promoting enterprise partnerships between programs and operations.
- Define the organization's risk appetite and communicate what it means across the entity, so there is common understanding of the why, what, who and when.
- Define the roles and operating practices of governance, education, accountability, and transparency over fraud risk.
- Establish fraud risk maturity models, covering areas such as:
  - Leadership
  - Legislation and regulation
  - Ethics
  - Risk strategy and appetite
  - Risk governance
  - Risk culture
  - Risk assessment and measurement
  - Risk management and monitoring, including prevention, detection, investigation and remediation programs and identification of emerging, changing and long-tailed fraud risks
  - Risk reporting and insights
  - Data and technology
- Develop approaches and tools to address common fraud risks in government, such fraud involving:
  - Procurement and contracting
  - Grants
  - Healthcare fraud
  - Social Security
  - Benefit programs, such as UI, student financial aid, and agricultural subsidies
  - Credit — loans and loan guarantees
  - Logistics and supply chain
  - Purchase and travel cards
  - Improper payments, including vendor payments
  - Disaster relief fraud
  - Financial reporting fraud
  - Tax evasion and fraudulent tax returns
  - Appropriation accounting
  - Identity fraud
  - Public corruption
  - Cyber
- Develop fraud oversight models, such as (1) performance metrics and reporting; (2) continuous monitoring and analysis, using ever-more sophisticated algorithms, predictive tools, and data analytics; and (3) audits and investigations.

Additional Government-Centric Fraud Risk Management Guidance is Available.

Our research identified additional fraud risk management guidance tailored to government, which will be valuable to governments globally as they establish Fraud Risk Management Programs or work to strengthen existing programs. Notable is the program in Australia and its *Fraud Control in Australian Government Entities – Better Practice Guide*, dated March 2011. The Australian guide comprehensively addresses fraud risk management in a government environment covering:

- The why, what, and who
- Leadership and culture
- Legislation, governance, and policy
- Fraud control strategies, including key fraud themes and government program management.
- Fraud prevention, including prevention measures and building fraud prevention into government program design
- Fraud detection, including passive and active detection measures and building detection into government program design
- Fraud response, including investigation and response in program delivery
- Monitoring, evaluation and reporting, including doing so in a government program context.
- Identity fraud, including Australia's national identity security strategy, law enforcement initiatives and identity fraud risk management options

Finally, the Australian guide contains appendices, which include:

- The legislative and policy framework for fraud risk management in Australia
- Questions an audit committee may wish to ask about a government Fraud Risk Management Program
- An example of a fraud risk register
- Audits by the Australian National Audit Office related to fraud control
- Sources used in developing the Australian guide

Other additional guidance that should be of use in considering a fraud risk program in the government environment include:

- *Australian Government Commonwealth Fraud Control Guidelines*
- *Approaches for Establishing Fraud Risk Assessment Programs and Conducting Fraud Audit Risk Assessments Within the Department of Defense*
- *European Commission Fraud Risk Assessment and Effective and Proportionate Anti-Fraud Measures.*
- *HM Treasury Fraud and the Government Internal Auditor*
- *National Treasury Republic of South Africa Public Sector Risk Management Framework*
- *UK Local Government Association Managing the Risk of Procurement Fraud*
- *Scottish Public Finance Manual: Fraud*
- *CIPFA Code of Practice on Managing the Risk of Fraud and Corruption*
- *CIPFA Better Governance Forum Managing the Risk of Fraud*
- *Office of New York State Comptroller Management's Responsibility for Internal Controls*
- *CIMA Fraud Risk Management: A Guide to Good Practice*
- *OCC Bulletin 2019-37, Operational Risk: Fraud Risk Management Principles*
- *Government of Canada: Guide to Integrated Risk Management*
- *Guide on Managing Fraud Risks at the Office of the Auditor General of Canada*
- *NIST Risk Management Framework*
- *Queensland Audit Office – Fraud Risk Assessment Tool*
- *USAID Public Financial Management Risk Assessment Framework Manual*
- *Association of Federal Enterprise Risk Management – Federal ERM Areas of Practice Guidance – 2021*
- *United Nations Office on Drugs and Crime – A Practical Guide to Corruption Risk Assessment and Management In Public Organizations – 2020*

[30] OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, section 270.24 to 270.29.

ABOUT COSO

Originally formed in 1985, COSO is a joint initiative of five private-sector organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).

ABOUT ACFE

Founded in 1988 by Dr. Joseph T. Wells, CFE, CPA, the Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organization and premier provider of anti-fraud training and education. Together with more than 90,000 members, the ACFE is reducing business fraud worldwide and inspiring public confidence in the integrity and objectivity within the profession.

The ACFE unites and supports the global anti-fraud community by providing educational tools and practical solutions for professionals through events, publications, networking, and educational materials for colleges and universities.

CERTIFIED FRAUD EXAMINERS

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

MEMBERSHIP

Members of the ACFE include accountants, internal auditors, fraud investigators, law enforcement officers, lawyers, business leaders, risk/compliance professionals, and educators, all of whom have access to expert training, educational tools, and resources. Whether their career is focused exclusively on preventing and detecting fraudulent activities or they just want to learn more about fraud, the ACFE provides anti-fraud professionals with the essential tools and resources necessary to accomplish their objectives.
To learn more, visit ACFE.com or call (800) 245-3321 / +1 (512) 478-9000.

CONTACT
Association of Certified Fraud Examiners
Global Headquarters
716 West Ave | Austin, TX 78701-2727 | USA
Phone: (800) 245-3321 | +1 (512) 478-9000
ACFE.com | info@ACFE.com

Testimonials

"The Guide is a great resource for professionals who appreciate the need to take a holistic approach to fraud risk management."

Todd DeZoort, Ph.D., CFE, NACD.DC
Durr-Fillauer Chair in Business Ethics and Professor of Accounting
Culverhouse School of Accountancy, The University of Alabama

"As much as we don't like to think about it, fraud is just part of the business landscape and human condition. Pressure, greed, insecurity, and many other emotions are involved which unfortunately fuel intentional bad behavior and decision-making. This guide expands upon Principle 8 in the 2013 COSO *Internal Control — Integrated Framework* in an effective way to help all organizations regardless of size, industry, form, or ownership more effectively address the unwelcome subject of fraud. Boards, management, accountants, internal auditors, and others will benefit from its advice, structure, and guidance."

Robert B. Hirth, Jr.
Senior Managing Director, Protiviti
COSO Chair Emeritus (2013–2018)

"Being a CPA as well as a CFE, I was already familiar with COSO guidance. Coupling that with a fraud risk management perspective is ideal for anyone in a corporate role. The FRMG provides clear direction for identifying and addressing risks, and makes it easy to integrate with overall corporate risk management efforts."

Valerie Scarantino
UGI Corporation

"I found the Guide to be a cost effective and valuable resource for fighting fraud as it approaches fraud prevention and detection on a comprehensive basis as opposed to piecemeal, which as is often the approach used by most organizations. Proactiveness vs. reactiveness is both more cost effective as well as protecting from something you can never recover from, reputation damage…the true cost of fraud. Unfortunately, many organizations fall into the "comfortable in action mode," in other words "it can't happen here," or simply don't know where or how to start a comprehensive, all-encompassing approach to fraud protection and detection. You now have a tool and resource to guide you through this process!"

Joseph M. Palmar, CPA, CFE, CFF
Chief Executive Officer
Palmar Forensics

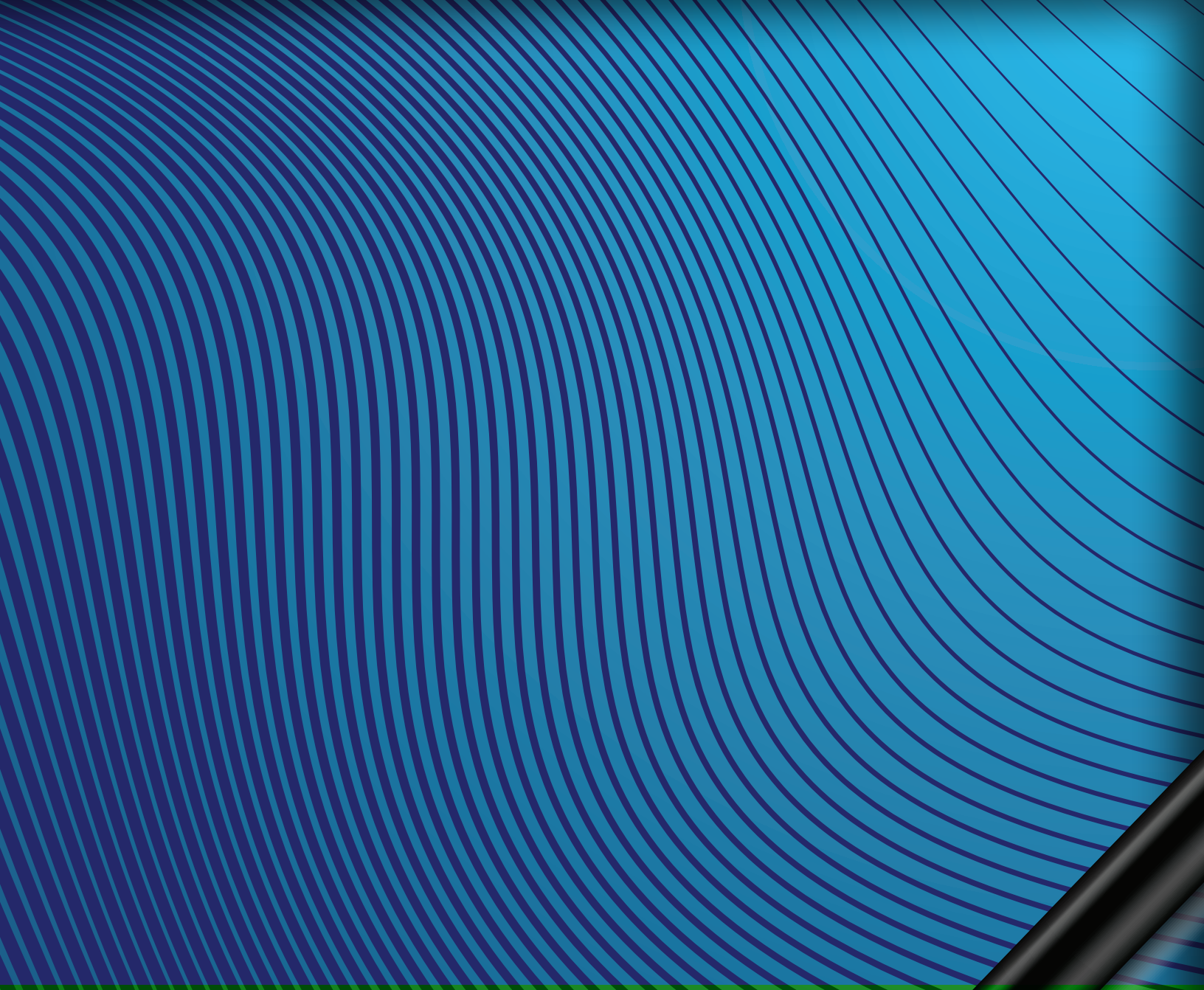
FRAUD RISK MANAGEMENT GUIDE

Second Edition

COSO

Committee of Sponsoring Organizations of the Treadway Coåmmission

ACFE
Association of Certified Fraud Examiners



FRAUD RISK MANAGEMENT GUIDE

Second Edition

COSO

Committee of Sponsoring Organizations of the Treadway Coåmmission

ACFE

Association of Certified Fraud Examiners