Dear Colleague,

Can fraud happen here? Will it happen again?

No self-respecting CEO wants fraud to occur in his or her organization. But can it happen? How vulnerable are we to fraud risks? What have we done to mitigate the risk? Are our mitigation techniques working?

In today’s business environment questions such as these are being pondered as the pressure mounts on organizations to be more accountable for proactively addressing fraud risks.

Why is fraud risk management so important? The reasons to pay attention to fraud risk include:

• Fraud occurs everywhere, and no organization is immune to its potential for damage or even devastation. In fact, research shows that fraud perpetrators are usually insiders and normally well respected, highly placed, experienced, tenured, and good performers.
• Recent history reveals that fraud is not discriminating. It can reap unimaginable havoc — regardless of size or industry — originating anywhere from the mailroom to the board room and ultimately bringing a company to its knees (e.g., home loan fraud, trading frauds, financial reporting frauds).
• Today's changing business environment includes globalization, technological advances, broad availability of information, and economic uncertainty. Communities, regulators, and investment markets expect organizations to catch major fraud and deal with it in a timely manner.
• Understanding vulnerabilities can help organizations deal with risks effectively and economically.
• Preventing and deterring fraud is significantly less costly than confronting the financial, operational, and reputational repercussions that can result from fraud.

Over the past 18 months a group of 21 thought leaders in the fraud risk management area have worked together to develop a paper titled, Managing the Business Risk of Fraud: A Practical Guide, through a joint project sponsored by The Institute of Internal Auditors, the American Institute of Certified Public Accountants, and the Association of Certified Fraud Examiners. The guide is designed to provide:

• Five key principles for proactively establishing an environment to effectively manage an organization’s fraud risks.
• A framework to assess fraud risks using an organized approach to planning, identifying, prioritizing, mitigating, monitoring, and dealing with fraud risk. This includes suggested roles and responsibilities for key players.
• Tools for writing a fraud policy, performing a risk assessment, identifying potential fraud risks, monitoring fraud risks, and setting up investigation protocols to handle fraud allegations as well as references to other sources for more information.
• Agreed upon recommendations for managing fraud risk from numerous experts in the field brought together in one document.
• Real-life examples of how fraud risk management principles are applied.
The guide can be used to help you build awareness of fraud risks within your organization, make assignments of responsibility, verify that your information about fraud risks is current and accurate, and ensure that your organization’s vulnerabilities to fraud are addressed properly. It also will demonstrate how you can access the knowledge and experience of existing in-house and consultative experts — such as internal auditors, enterprise risk management specialists, and external auditors — to strengthen your fraud risk management efforts.

Managing the Business Risk of Fraud: A Practical Guide is available for free downloading from:

The IIA at www.theiia.org/managingfraudrisk
The AICPA at http://fvs.aicpa.org/fraudriskguide
The ACFE at www.acfe.com/guidancepaper/guidancepaper.asp

It is the belief of all who participated in this important project that, together, we can make a difference in today’s business community by better managing the risks associated with fraud. On behalf of our collective stakeholders, we invite you to join us in this initiative by carefully reviewing the guide, discussing it in detail with your management team and board, and evaluating your current practices in comparison with the principles provided.

This executive summary is for your reference and convenience. We hope it sufficiently emphasizes the importance of the information included in the full guide. Please feel free to contact us if we can be of any further assistance or if you have any questions about how to use Managing the Business Risk of Fraud: A Practical Guide.

Sincerely,

David A. Richards, CIA
President
The Institute of Internal Auditors

Barry C. Melancon, CPA
President and Chief Executive Officer
American Institute of Certified Public Accountants

James D. Ratley, CFE
President
Association of Certified Fraud Examiners
PROJECT MANAGER

David A. Richards, CIA
President
The Institute of Internal Auditors

TEAM MEMBERS

Toby J.F. Bishop, CPA, CFE, FCA
Director, Deloitte Forensic Center
Deloitte Financial Advisory Services LLP

Corey Anne Bloom, CA, CA•IFA, CFE
Senior Associate, Dispute Resolution and Financial Investigation Services
RSM Richter Inc.

Joseph V. Carcello, Ph.D., CIA, CPA, CMA
Director of Research, Corporate Governance Center
Ernst & Young Professor
University of Tennessee

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

Holly Daniels, CIA, CISA
Technical Director, Standards and Guidance
The Institute of Internal Auditors

Ronald L. Durkin, CPA, CFE, CIRA
National Partner-in-Charge, Fraud and Misconduct Investigations
KPMG LLP

David J. Elzinga, CA•IFA, CFE
Partner, Forensic Accounting and Investigation Services
Grant Thornton LLP

Robert E. Farrell, CFE
Principal
White Collar Investigations

Bruce J. Gavioli, CPA, MBA
Partner
Deloitte Financial Advisory Services LLP

John D. Gill, JD, CFE
Research Director
Association of Certified Fraud Examiners

Sandra K. Johnigan, CPA, CFE
Johnigan, P.C.

Thomas M. Miller, CPA/ABV, CFE, PI
Technical Manager, Forensic and Valuation Services
AICPA

Lynn Morley, CIA, CGA
Morley Consulting & Training Services Inc.

Thomas Sanglier
Partner
Ernst & Young LLP

Jeffrey Steinhoff
Managing Director, Financial Management and Assurance (Retired)
United States Government Accountability Office

William E. Stewart
Partner, Fraud Investigation and Dispute Services
Ernst & Young LLP

Bill Warren
Director, Fraud Risks and Controls
PricewaterhouseCoopers LLP

Mark F. Zimbelman, Ph.D.
Associate Professor and Selvoy J. Boyer Fellow
Brigham Young University

PROJECT ADVISERS

Eleanor Bloxham
Chief Executive Officer
The Value Alliance and Corporate Governance Alliance

Larry Harrington
Vice President, Internal Audit
Raytheon Company
FROM THE SPONSORING ORGANIZATIONS

The views expressed in this document are for guidance purposes only and are not binding on organizations. Organizations should design and implement policies and procedures that best suit them. The IIA, AICPA, and ACFE shall not be responsible for organizations failing to establish required policies and procedures that best suit their needs. This guide is intended to be applicable globally but heavily references practices in the United States and, where available, also provides references to information from other countries.

The Institute of Internal Auditors
David A. Richards, CIA
President

American Institute of Certified Public Accountants
Barry C. Melancon, CPA
President and Chief Executive Officer

The Association of Certified Fraud Examiners
James D. Ratley, CFE
President

ENDORSERS

The endorsing organizations support the nonbinding guidance of this guide as being of use to management and organizations interested in making fraud risk management programs work. The views and conclusions expressed in this guide are those of the authors and have not been adopted, approved, disapproved, or otherwise acted upon by a committee, governing body, or the membership of the endorsers, which includes:

California Society of Certified Public Accountants
Chartered Accountants of Canada
Institute of Management Accountants
Open Compliance and Ethics Group
Society of Corporate Compliance and Ethics
The Association of Chartered Certified Accountants
The Value Alliance
**MANAGING THE BUSINESS RISK OF FRAUD: A PRACTICAL 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.¹

**INTRODUCTION**

All organizations are subject to fraud risks. Large frauds have led to the downfall of entire organizations, massive investment losses, significant legal costs, incarceration of key individuals, and erosion of confidence in capital markets. Publicized fraudulent behavior by key executives has negatively impacted the reputations, brands, and images of many organizations around the globe.

Regulations such as the 1977 U.S. Foreign Corrupt Practices Act, the 1997 Organization for Economic Co-operation and Development Anti-Bribery Convention, the U.S. Sarbanes-Oxley Act of 2002, the 2005 U.S. Federal Sentencing Guidelines, and similar legislation throughout the world have increased management’s responsibility of fraud risk management.

Reactions to recent corporate scandals have led the public and stakeholders to expect organizations to take a “no-fraud tolerance” attitude. Good governance principles demand that an organization’s board of directors, or equivalent oversight body, ensure overall high ethical behavior in any organization, regardless of its status as public, private, government, or not-for-profit; its relative size; or its industry. The board’s role is critical because historically, most major frauds are perpetrated by senior management in collusion with other employees.² Vigilant handling of fraud cases within an organization sends clear signals to the public, stakeholders, and regulators about the board and management’s attitude toward fraud risks and about the organization’s fraud risk tolerance.

In addition to the board, personnel at all levels of the organization — including every level of management, staff, and internal auditors, as well as the organization’s external auditors — are responsible for dealing with fraud risk. Particularly, they are expected to explain how the organization is responding to heightened regulations and public and stakeholder scrutiny; what form of fraud risk management program the organization has in place and how they identify fraud risks; what they are doing to better prevent fraud, or at least detect it sooner; and what process is in place to investigate fraud and take corrective action.³ This guide is designed to help address these tough issues.

¹ This definition of fraud was developed uniquely for this paper, and the authors recognize that many other definitions of fraud exist, including those developed by the sponsoring organizations and endorsers of this paper.

² Refer to The Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) 1999 analysis of cases of fraudulent financial statements investigated by the U.S. Securities and Exchange Commission (SEC).

This guide also recommends ways in which boards, senior management, and internal auditors can fight fraud in their organization. Specifically, it provides credible guidance from leading professional organizations that defines principles and theories for fraud risk management and describes how organizations of various sizes and types can establish their own fraud risk management program. The guide includes examples of key program components and resources that an organization can use as a starting point to effectively and efficiently develop a fraud risk management program. Each organization needs to assess the degree of emphasis to place on fraud risk management based on its size and circumstances.

**SUMMARY**

As noted, 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. Regardless of culture, ethnicity, religion, or other factors, certain individuals will be motivated to commit fraud. A 2007 Oversight Systems study discovered that the primary reasons why frauds occur are “pressures to do ‘whatever it takes’ to meet goals” (81 percent of respondents) and “to seek personal gain” (72 percent). Additionally, many respondents indicated that “they do not consider their actions fraudulent” (40 percent) as a reason for wrongful behavior.

Only through diligent and ongoing effort can an organization protect itself against significant acts of fraud. Key principles for proactively establishing an environment to effectively manage an organization’s fraud risk include:

**Principle 1:** As part of an organization’s governance structure, a fraud risk management program should be in place, including a written policy (or policies) to convey the expectations of the board of directors and senior management regarding managing fraud risk.

**Principle 2:** Fraud risk exposure should be assessed periodically by the organization to identify specific potential schemes and events that the organization needs to mitigate.

**Principle 3:** Prevention techniques to avoid potential key fraud risk events should be established, where feasible, to mitigate possible impacts on the organization.

**Principle 4:** Detection techniques should be established to uncover fraud events when preventive measures fail or unmitigated risks are realized.

**Principle 5:** A reporting process should be in place to solicit input on potential fraud, and a coordinated approach to investigation and corrective action should be used to help ensure potential fraud is addressed appropriately and timely.

---

4 Throughout this paper, the terms “board” and “board of directors” refer to the governing body 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.


6 Fraud risk management programs, also known as antifraud programs, can take many forms, as noted in Section 1 (Fraud Risk Governance) under the Fraud Risk Management Program heading.
The following is a synopsis of the contents contained in the full guide, which provides practical evidence for organizations committed to preserving stakeholder value. The guide can be used to assess an organization’s fraud risk management program, as a resource for improvement, or to develop a program where none exists.

**Fraud Risk Governance**

Organization stakeholders have clearly raised expectations for ethical organizational behavior. Meanwhile, regulators worldwide have increased criminal penalties that can be levied against organizations and individuals who participate in committing fraud. Organizations should respond to such expectations, and effective governance processes are the foundation of fraud risk management. Lack of effective corporate governance seriously undermines any fraud risk management program. Also, the organization’s overall tone at the top sets the standard regarding its tolerance of fraud.

The board of directors should ensure that its own governance practices set the tone for fraud risk management and that management implements policies that encourage ethical behavior, including processes for employees, customers, and vendors to report instances where those standards are not met. The board should also monitor the organization’s fraud risk management effectiveness, which should be a regular item on its agenda. To this end, the board should appoint one executive-level member of management to be responsible for coordinating fraud risk management and reporting to the board on the topic.

Most organizations have some form of written policies and procedures to manage fraud risks. However, few have developed a concise summary of these activities and documents to help them communicate and evaluate their processes. We refer to the aggregate of these as the fraud risk management program, even if the organization has not formally designated it as such.

While each organization needs to consider its size and complexity when determining what type of formal documentation is most appropriate, the following elements should be found within a fraud risk management program:

- Roles and responsibilities.
- Commitment.
- Fraud awareness.
- Affirmation process.
- Conflict disclosure.
- Fraud risk assessment.
- Reporting procedures and whistleblower protection.
- Investigation process.
- Corrective action.
- Quality assurance.
- Continuous monitoring.
Roles and Responsibilities

To help ensure an organization’s program remains effective, it is important to understand the roles and responsibilities of personnel at all levels of the organization with respect to fraud risk management.

Policies, job descriptions, charters, and delegations of authority should define roles and responsibilities related to the fraud risk management program. In particular, the documentation should articulate who is responsible for the governance oversight of fraud control (i.e., the role and responsibility of the board of directors and/or designated committee of the board). Documentation also should reflect management’s responsibility for the design and implementation of the fraud risk strategy, and how different segments of the organization support the fraud risk management program. Fraud risk management often will be supported by risk management, compliance, general counsel, the ethics office, security, information technology, and internal auditing or their equivalents. The board of directors, audit committee, management, staff, and internal auditing all have key roles in an organization’s fraud risk management program.

Board of Directors

The board has the responsibility to ensure that management designs effective fraud risk management documentation to encourage ethical behavior and empower employees, customers, and vendors to insist those standards are met every day. The board should:

- Understand fraud risks.
- Maintain oversight of the fraud risk assessment by ensuring that fraud risk has been considered as part of the organization’s risk assessment and strategic plans. This responsibility should be addressed under a periodic agenda item at board meetings when general risks to the organization are considered.
- Monitor management’s reports on fraud risks, policies, and control activities, which includes obtaining assurance that the controls are effective. The board also should establish mechanisms to ensure it is receiving accurate and timely information from management, employees, internal and external auditors, and other stakeholders regarding potential fraud occurrences.
- Oversee the internal controls established by management.
- Set the appropriate tone at the top through the CEO’s job description, hiring, evaluation, and succession-planning processes.
- Have the ability to retain outside experts where needed.
- Provide external auditors with evidence regarding the board’s active involvement and concern about fraud risk management.

The board may choose to delegate oversight of some or all of such responsibilities to a committee of the board. These responsibilities should be documented in the board and applicable committee charters. The board should ensure it has sufficient resources of its own and approve
sufficient resources in the budget and long-range plans to enable the organization to achieve its fraud risk management objectives.

**Audit Committee (Or Similar Oversight Body)**

An audit committee of the board that is committed to a proactive approach to fraud risk management maintains an active role in the oversight of the organization’s assessment of fraud risks, and uses internal auditors, or other designated personnel, to monitor fraud risks.

At each meeting the audit committee should confer separately with appropriate individuals, such as the chief internal audit executive and senior financial person. The audit committee should understand how internal and external audit strategies address fraud risk and should not only focus on what the auditors are doing to detect fraud, but also on what management is doing to prevent fraud, where possible.

The audit committee should be aware that the organization’s external auditors have a responsibility to plan and perform the audit of the organization’s financial statements to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. The extent and limitations of an external audit are generally governed by the applicable audit standards in place. The audit committee should insist on openness and honesty with the external auditors, and the external auditors also should have commitment and cooperation from the committee. This includes open and candid dialogue between the audit committee and the external auditors regarding the committee’s knowledge of any fraud or suspected fraud affecting the organization, as well as how the audit committee exercises oversight activities with respect to the organization’s assessment of the risks of fraud and the programs and controls established to mitigate these risks.

**Management**

Management has overall responsibility for the design and implementation of a fraud risk management program, including:

- Setting the tone at the top for the rest of the organization. As mentioned, an organization’s culture plays an important role in preventing, detecting, and deterring

---

7 This section discusses more detailed governance roles using the audit committee as an illustration. Some organizations may require this level of responsibility by the full board, or the board may delegate it to a risk management committee, strategic planning committee, etc. Accounting standards and securities regulations in each country provide more detailed guidance as to best practices or legal requirements in their jurisdictions.

8 The inherent limitations of an external audit regarding matters related to fraud are described in applicable audit standards. The standards acknowledge that owing to the inherent limitations of an external audit, there is an unavoidable risk that some material misstatements of the financial statements — particularly those resulting from fraud — will not be detected, even though the external auditor has properly planned and performed in accordance with generally accepted standards.

fraud. Management needs to create a culture through words and actions where 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.

- Implementing adequate internal controls — including documenting the fraud risk management policies and procedures and evaluating their effectiveness — that are aligned with the organization’s fraud risk assessment. To conduct a reasonable evaluation, it is necessary to compile information from various areas of the organization as part of the fraud risk management program.
- Reporting to the board on what actions have been taken to manage fraud risks and regularly reporting on the effectiveness of the fraud risk management program. This includes reporting any remedial steps that are needed as well as reporting actual frauds.

Staff
Strong controls against fraud are the responsibility of everyone in the organization.

All levels of staff, including management, should:

- Have a basic understanding of fraud and be aware of the red flags.
- Understand their roles within the internal control framework. Staff members should understand how their job procedures are designed to manage fraud risks and when noncompliance may create an opportunity for fraud to occur or go undetected.
- Read and understand policies and procedures, such as the fraud policy, code of conduct, and whistleblower policy, as well as other operational policies and procedures, such as procurement manuals.
- As required, participate in the process of creating a strong control environment and designing and implementing fraud control activities, as well as participate in monitoring activities.
- Report suspicions or incidences of fraud.
- Cooperate in investigations.

Internal Auditing
Internal auditing should provide objective assurance to the board and management that fraud controls are sufficient for identified fraud risks and ensure that the controls are functioning effectively. Internal auditors may review the comprehensiveness and adequacy of the risks identified by management — especially in regards to management override risks.¹⁰

---

¹⁰ Refer to AICPA’s Management Override of Internal Controls: The Achilles’ Heel of Fraud Prevention publication.
Internal auditors should consider the organization’s assessment of fraud risk when developing their annual audit plan and review management’s fraud management capabilities periodically. When performing engagements, internal auditors should devote adequate time and attention to evaluating the design and operation of internal controls related to fraud risk management. They should exercise professional skepticism when reviewing activities to be on guard for the signs of fraud. Potential frauds uncovered during an engagement should be treated in accordance with a well-defined response plan consistent with professional and legal standards. Internal auditing should also take an active role in support of the organization’s ethical culture.\textsuperscript{11}

Internal auditing should be independent (authority and reporting relationships), have adequate access to the audit committee, and adhere to professional standards.

**Fraud Risk Assessment**

To protect itself and its stakeholders from fraud effectively and efficiently, an organization should understand fraud risk and the specific risks that directly or indirectly apply to the organization. A structured fraud risk assessment, tailored to the organization’s size, complexity, industry, and goals, should be performed and updated periodically. The assessment may be integrated with an overall organizational risk assessment or a stand-alone exercise, but should, at a minimum, include risk identification, a risk likelihood and significance assessment, and risk response.

An effective fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud. Employee incentive programs and the metrics on which they are based can provide a map to where fraud is most likely to occur. Fraud risk assessment should consider the potential override of controls by management as well as areas where controls are weak or there is a lack of segregation of duties.

Individual organizations will have different risk tolerances. Fraud risks can be addressed by establishing practices and controls to mitigate the risk, accepting the risk — but monitoring actual exposure — or designing ongoing or specific fraud evaluation procedures to deal with individual fraud risks. An organization should strive for a structured approach versus a haphazard approach. The benefit an implemented fraud risk management program provides should exceed its cost. Management and board members should ensure the organization has the appropriate control mix in place, recognizing their oversight duties and responsibilities in terms of the organization’s sustainability and their role as fiduciaries to stakeholders, depending on organizational form. Management is responsible for developing and executing mitigating controls to address fraud risks while ensuring controls are executed efficiently by competent and objective individuals.

\textsuperscript{11} Refer to IIA Practice Advisory 2130-1: Role of the Internal Audit Activity and Internal Auditor in the Ethical Culture of an Organization.
**Fraud Prevention and Detection**

Fraud prevention and detection are related, but are not the same concepts. Prevention encompasses policies, procedures, training, and communication that stop fraud from occurring; whereas detection focuses on activities and techniques that timely recognize whether fraud has occurred or is occurring.

While preventive techniques do not ensure fraud will not be committed, they are the first line of defense in minimizing fraud risk. One key to prevention is expanding from the board down throughout the organization an awareness of the fraud risk management program, including the types of fraud that may occur.

Meanwhile, one of the strongest fraud deterrents is the awareness that effective detective controls are in place. Combined with preventive controls, detective controls enhance the effectiveness of a fraud risk management program by demonstrating that preventive controls are working as intended and identifying fraud if it does occur. Although detective controls may provide evidence that fraud has occurred or is occurring, they are not intended to prevent fraud.

Every organization is susceptible to fraud, but not all fraud can be prevented, nor is it cost-effective to try. An organization may determine it is more cost-effective to design its controls to detect, rather than prevent, certain fraud schemes. It is important that organizations consider both fraud prevention and fraud detection.

**Investigation and Corrective Action**

No system of internal control can provide absolute assurance against fraud. As a result, the board should ensure the organization develops a system for prompt, competent, and confidential review, investigation, and resolution of noncompliance and allegations involving potential fraud. The board should also define its own role in the investigation process. An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation by establishing and preplanning investigative and corrective action processes.

The board and the organization should establish a process to evaluate allegations. Individuals assigned to investigations should have the necessary authority and skills to evaluate the allegation and determine the appropriate course of action. The process should include a tracking or case management system where all allegations of fraud are logged. Clearly, the board should be actively involved with respect to allegations involving senior management.

If further investigation is deemed appropriate as the next course of action, the board should ensure that the organization has an appropriate and effective process to investigate cases and maintain confidentiality. A consistent process for conducting investigations can help the organization mitigate losses and manage risk associated with the investigation. In accordance with policies approved by the board, the investigation team should report its findings to the appropriate party, such as senior management, directors, legal counsel, and oversight bodies. Public disclosure may also need to be made to law enforcement, regulatory bodies, investors, shareholders, the media, or others.
Thus, to properly address fraud risk within the organization, the principles described in this paper are needed to make sure:

- Suitable fraud risk management oversight and expectations exist (i.e., governance) — Principle 1.
- Fraud exposures are identified and evaluated (i.e., risk assessment) — Principle 2.
- Appropriate processes and procedures are in place to manage these exposures (i.e., prevention and detection) — Principles 3 and 4.
- Fraud allegations are addressed and appropriate corrective action is taken in a timely manner (i.e., investigation and corrective action) — Principle 5.


The full text of the guidance paper includes references to key publications and guidance, examples of potential fraud risks, and sample forms for risk assessment and evaluation of fraud risk management programs, plus full discussion of each of the five principles noted above.