SPONSORED BY:

The Institute of Internal Auditors

The American Institute of Certified Public Accountants

Association of Certified Fraud Examiners

Managing the Business Risk of Fraud: A Practical Guide

FROM THE SPONSORING ORGANIZATIONS:

The Institute of Internal Auditors
David A. Richards, CIA, CPA
President and Project Manager

The American Institute of Certified Public Accountants
Barry C. Melancon, CPA
President and CEO

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

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 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, provides references to information from other countries, as well. We anticipate further references will be included in future updates.

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 U.S. Foreign Corrupt Practices Act of 1977 (FCPA), the 1997 Organisation for Economic Co-operation and Development Anti-Bribery Convention, the U.S. Sarbanes-Oxley Act of 2002, the U.S. Federal Sentencing Guidelines of 2005, and similar legislation throughout the world have increased management's responsibility for 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 the organization, regardless of its status as public, private, government, or not-for-profit; its relative size; or its industry. The board's role is critically important 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 — have responsibility for dealing with fraud risk. Particularly, they are expected to explain how the organization is responding to heightened regulations, as well as public and stakeholder scrutiny; what form of fraud risk management program the organization has in place; how it identifies fraud risks; what it is doing to better prevent fraud, or at least detect it sooner; and what process is in place to investigate fraud and take corrective action[3]. This guide is designed to help address these tough issues.

This guide recommends ways in which boards[4], 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

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

[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).

[3] Refer to June 2007 SEC *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934* and U.S. Public Company Accounting Oversight Board (PCAOB) Auditing Standard No. 5 (AS5), An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements, for comments on fraud responsibilities.

[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.

establish their own fraud risk management program. 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. Each organization needs to assess the degree of emphasis to place on fraud risk management based on its size and circumstances.

EXECUTIVE 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[5] discovered that the primary reasons why fraud occurs 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[6] 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.**

The following is a summary of this guide, which provides practical evidence for organizations committed to preserving stakeholder value. This 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

[5] The 2007 Oversight Systems Report on Corporate Fraud, www.oversightsystems.com.

[6] Fraud risk management programs, also known as anti-fraud programs, can take many forms, as noted in Section 1 (Fraud Risk Governance) under the Fraud Risk Management Program heading.

who participate in committing fraud. Organizations should respond to such expectations. Effective governance processes are the foundation of fraud risk management. Lack of effective corporate governance seriously undermines any fraud risk management program. 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, vendors, and other third parties 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.

Fraud Risk Assessment

To protect itself and its stakeholders effectively and efficiently from fraud, 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 performed as a stand-alone exercise, but should, at a minimum, include risk identification, risk likelihood and significance assessment, and risk response.

Fraud risk identification may include gathering external information from regulatory bodies (e.g., securities commissions), industry sources (e.g., law societies), key guidance setting groups (e.g., Cadbury, King Report[7], and The Committee of Sponsoring Organizations of the Treadway Commission (COSO)), and professional organizations (e.g., The Institute of Internal Auditors (IIA), the American Institute of Certified Public Accountants (AICPA), the Association of Certified Fraud Examiners (ACFE), the Canadian Institute of Chartered Accountants (CICA), The CICA Alliance for Excellence in Investigative and Forensic Accounting, The Association of Certified Chartered Accountants (ACCA), and the International Federation of Accountants (IFAC), plus others noted in Appendix A of this document). Internal sources for identifying fraud risks should include interviews and brainstorming with personnel representing a broad spectrum of activities within the organization, review of whistleblower complaints, and analytical procedures.

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.

The speed, functionality, and accessibility that created the enormous benefits of the information age have also increased an organization's exposure to fraud. Therefore, any fraud risk assessment should consider access and override of system controls as well as internal and external threats to data integrity, system security, and theft of financial and sensitive business information.

Assessing the likelihood and significance of each potential fraud risk is a subjective process that should consider not only monetary significance, but also significance to an organization's financial reporting, operations, and reputation, as well as legal and regulatory compliance requirements. An initial assessment of fraud risk should consider the inherent risk[8] of a particular fraud in the absence of any known controls that may address the risk.

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.

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 promptly recognize timely whether fraud has occurred or is occurring.

---

[7] The Cadbury Report refers to *The Report of the Committee on the Financial Aspects of Corporate Governance*, issued by the United Kingdom on Dec. 10, 1992 and the King Report refers to the *King Report on Corporate Governance for South Africa*, issued in 1994.

[8] Inherent risk is the risk before considering any internal controls in place to mitigate such risk.

While prevention 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 promoting 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 by 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 instances 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 investigation 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.

If certain actions are required before the investigation is complete to preserve evidence, maintain confidence, or mitigate losses, those responsible for such decisions should ensure there is sufficient basis for those actions. When access to computerized information is required, specialists trained in computer file preservation should be used. Actions taken should be appropriate under the circumstances, applied consistently to all levels of employees (including senior management), and taken only after consultation with human resources (HR) and individuals responsible for such decisions. Consulting legal counsel is also strongly recommended before undertaking an investigation and is critical before taking disciplinary, civil, or criminal action. As a matter of good governance, management and the board should ensure that the foregoing measures are in place.

FISCAL MANAGEMENT GOALS AND OBJECTIVES
FINANCIAL ETHICS

All Trustees, employees, vendors, contractors, agents, consultants, volunteers, and any other parties who are involved in the District's financial transactions shall act with integrity and diligence in duties involving the District's fiscal resources.

Note: See the following policies and/or administrative regulations regarding conflicts of interest, ethics, and financial oversight:

- Code of ethics:
  for Board members—BBF
  for employees—DH
- Financial conflicts of interest:
  for public officials—BBFA
  for all employees—DBD
  for vendors—CHE
- Compliance with state and federal grant and award requirements: CB, CBB
- Financial conflicts and gifts and gratuities regarding federal funds: CB, CBB
- Systems for monitoring the District's investment program: CDA
- Budget planning and evaluation: CE
- Compliance with accounting regulations: CFC
- Activity fund management: CFD
- Criminal history record information for employees: DBAA, DC
- Disciplinary action for fraud by employees: DCD, DCE, and DF series

FRAUD AND FINANCIAL IMPROPRIETY

The District prohibits fraud and financial impropriety, as defined below, in the actions of its Trustees, employees, vendors, contractors, agents, consultants, volunteers, and others seeking or maintaining a business relationship with the District.

DEFINITION

Fraud and financial impropriety shall include but not be limited to:

1. Forgery or unauthorized alteration of any document or account belonging to the District.
2. Forgery or unauthorized alteration of a check, bank draft, or any other financial document.

3. Misappropriation of funds, securities, supplies, or other District assets, including employee time.
4. Impropriety in the handling of money or reporting of District financial transactions.
5. Profiteering as a result of insider knowledge of District information or activities.
6. Unauthorized disclosure of confidential or proprietary information to outside parties.
7. Unauthorized disclosure of investment activities engaged in or contemplated by the District.
8. Accepting or seeking anything of material value from contractors, vendors, or other persons providing services or materials to the District, except as otherwise permitted by law or District policy. [See CB, DBD]
9. Inappropriately destroying, removing, or using records, furniture, fixtures, or equipment.
10. Failure to provide financial records required by federal, state, or local entities.
11. Failure to disclose conflicts of interest as required by law or District policy.
12. Any other dishonest act regarding the finances of the District.
13. Failure to comply with requirements imposed by law, the awarding agency, or a pass-through entity for state and federal awards.

FINANCIAL CONTROLS AND OVERSIGHT

Each employee who supervises or prepares District financial reports or transactions shall set an example of honest and ethical behavior and shall actively monitor his or her area of responsibility for fraud and financial impropriety.

FRAUD PREVENTION

The Superintendent or designee shall maintain a system of internal controls to deter and monitor for fraud or financial impropriety in the District.

REPORTS

Any person who suspects fraud or financial impropriety in the District shall report the suspicions immediately to any supervisor, the Superintendent or designee, the Board President, or local law enforcement.

Reports of suspected fraud or financial impropriety shall be treated as confidential to the extent permitted by law. Limited disclosure may be necessary to complete a full investigation or to comply with

law. All employees involved in an investigation shall be advised to keep information about the investigation confidential.

PROTECTION FROM RETALIATION

Neither the Board nor any District employee shall unlawfully retaliate against a person who in good faith reports perceived fraud or financial impropriety. [See DG]

FRAUD INVESTIGATIONS

In coordination with legal counsel and other internal or external departments or agencies, as appropriate, the Superintendent, Board President, or a designee shall promptly investigate reports of potential fraud or financial impropriety.

RESPONSE

If an investigation substantiates a report of fraud or financial impropriety, the Superintendent or designee shall promptly inform the Board of the report, the investigation, and any responsive action taken or recommended by the administration.

If an employee is found to have committed fraud or financial impropriety, the Superintendent or designee shall take or recommend appropriate disciplinary action, which may include termination of employment. If a contractor or vendor is found to have committed fraud or financial impropriety, the District shall take appropriate action, which may include cancellation of the District's relationship with the contractor or vendor.

When circumstances warrant, the Board, Superintendent, or designee may refer matters to appropriate law enforcement or regulatory authorities. In cases involving monetary loss to the District, the District may seek to recover lost or misappropriated funds.

The final disposition of the matter and any decision to file a criminal complaint or to refer the matter to the appropriate law enforcement or regulatory agency for independent investigation shall be made in consultation with legal counsel.

FEDERAL AWARDS DISCLOSURE

The District shall disclose, in a timely manner in writing to the federal awarding agency or pass-through entity, all violations of federal criminal law involving fraud, bribery, or gratuity violations potentially affecting a federal grant award. [See CBB]

ANALYSIS OF FRAUD

After any investigation substantiates a report of fraud or financial impropriety, the Superintendent or designee shall analyze conditions or factors that may have contributed to the fraudulent or improper activity. The Superintendent or designee shall ensure that appropriate administrative procedures are developed and implemented to prevent future misconduct. These measures shall be presented to the Board for review.

Fraud Risk Assessment

For more information this excerpt from "Managing the Business Risk of Fraud: A Practical Guide", which was sponsored by The Institute of Internal Auditors is included. The complete report may be accessed via the internet at www.theiia.org.