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

The Institute of Internal Auditors

AICPA®

ACFE

Association of Certified Fraud Examiners

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.

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 & Misconduct Investigations
KPMG LLP

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

Robert E. Farrell, CFE
Principal, White Collar Investigations

Bruce J. Gavioli, CPA, MBA
Partner & National Leader, Anti-fraud Consulting
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)
U.S. Government Accountability Office

William E. Stewart
Partner, Fraud Investigation & 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 ADVISORS:

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

Larry Harrington
Vice President, Internal Audit
Raytheon Company

ENDORSERS:

The following organizations endorse 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 endorser.

MANAGING THE BUSINESS RISK OF FRAUD: A PRACTICAL GUIDE

TABLE OF CONTENTS PAGE

APPENDICES:

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.

Thus, to properly address fraud risk within the organization, principles described in the following sections of this paper are needed to make sure:

- Suitable fraud risk management oversight and expectations exist (governance) — Principle 1.
- Fraud exposures are identified and evaluated (risk assessment) — Principle 2.
- Appropriate processes and procedures are in place to manage these exposures (prevention and detection) — Principles 3 & 4.
- Fraud allegations are addressed, and appropriate corrective action is taken in a timely manner (investigation and corrective action) — Principle 5.[9]

SECTION 1: FRAUD RISK GOVERNANCE

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.

Corporate governance has been defined in many ways, including "The system by which companies are directed and controlled,"[10] and "The process by which corporations are made responsive to the rights and wishes of stakeholders."[11] Corporate governance is also the manner in which management and those charged with oversight accountability meet their obligations and fiduciary responsibilities to stakeholders.

Business stakeholders (e.g., shareholders, employees, customers, vendors, governmental entities, community organizations, and media) have raised the awareness and expectation of corporate behavior and corporate governance practices. Some organizations have developed corporate cultures that encompass strong board governance practices, including:

- Board ownership of agendas and information flow.
- Access to multiple layers of management and effective control of a whistleblower hotline.
- Independent nomination processes.
- Effective senior management team (including chief executive officer (CEO), chief financial officer, and chief operating officer) evaluations, performance management, compensation, and succession planning.
- A code of conduct specific for senior management, in addition to the organization's code of conduct.
- Strong emphasis on the board's own independent effectiveness and process through board evaluations, executive sessions, and active participation in oversight of strategic and risk mitigation efforts.

These corporate cultures also include board assurance of business ethics considerations in hiring, evaluation, promotion, and remuneration policies for employees as well as ethics considerations in all aspects of their relationships with customers, vendors, and other business stakeholders. Effective boards and organizations will also

[9] The Open Compliance and Ethics Group (OCEG) Foundation principles displayed in Appendix F of this document also provide guidance on underlying principles of good governance relative to fraud risk management.

[10] Sir Adrian Cadbury, The Committee on the Financial Aspects of Corporate Governance.

[11] Ada Demb and F. Friedrich Neubauer, *The Corporate Board: Confronting the Paradoxes.*

address issues of ethics and the impact of ethical behavior on business strategy, operations, and long-term survival. The level of board and corporate commitment to these areas varies widely and directly affects the fraud risk profile of an organization.

Effective business ethics programs can serve as the foundation for preventing, detecting, and deterring fraudulent and criminal acts. An organization's ethical treatment of employees, customers, vendors, and other partners will influence those receiving such treatment. These ethics programs create an environment where making the right decision is implicit.

The laws of most countries prohibit theft, corruption, and financial statement fraud. Government regulations worldwide have increased criminal penalties that can be levied against companies and individuals who participate in fraud schemes at the corporate level, and civil settlements brought by shareholders of public companies or lenders have rocketed to record amounts[12]. Market capitalizations of public companies drop dramatically at any hint of financial scandal, and likewise, customers punish those firms whose reputations are sullied by indications of harmful behavior. Therefore, it should be clear that organizations need to respond to such expectations, and that the board and senior management will be held accountable for fraud. In many organizations this is managed as part of corporate governance through entity-level controls, including a fraud risk management program[13].

ROLES AND RESPONSIBILITIES

To help ensure an organization's fraud risk management program effective, it is important to understand the roles and responsibilities that personnel at all levels of the organization have with respect to fraud risk management. Policies, job descriptions, charters, and/or delegations of authority should define roles and responsibilities related to fraud risk management. 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 should also reflect management's responsibility for the design and implementation of the fraud risk strategy, and how different segments of the organization support fraud risk management. Fraud risk management will often be supported by risk management, compliance, general counsel, the ethics office, security, information technology (IT), 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

To set the appropriate tone at the top, the board of directors first should ensure that the board itself is governed properly. This encompasses all aspects of board governance, including independent-minded board members who exercise control over board information, agenda, and access to management and outside advisers, and who independently carry out the responsibilities of the nominating/governance, compensation, audit, and other committees.

[12] In the United States and Europe, regulators assessed fines and penalties in excess of US $1 billion for fraudulent and/or criminal behavior during 2007. See www.sec.gov.

[13] ALARM (The National Forum for Risk Management in the Public Sector (UK)) lists a fraud risk management program as one of five essential governance strategies to manage fraud risk. Other strategies include a zero-tolerance culture, a sound counter-fraud and corruption framework, strong systems of internal control, and close working relationships with partners regarding fraud risk management activities.

The board also has the responsibility to ensure that management designs effective fraud risk management documentation to encourage ethical behavior and to 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 include 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 job description, hiring, evaluation, and succession-planning processes.
- Have the ability to retain and pay 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)[14]

The audit committee should be composed of independent board members and should have at least one financial expert, preferably with an accounting background. The committee should meet 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 controls. It is key that the audit committee receive regular reports on the status of reported or alleged fraud.

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. Such a committee also provides the external auditors with evidence that the committee is committed to fraud risk management and will discuss with the external auditor the auditors' planned approach to fraud detection as part of the financial statement audit. *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention*, an AICPA publication, provides valuable information for audit committees that take this approach.

[14] This heading 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 what is a best practice or legal requirement in their jurisdictions.

At each audit committee meeting, the committee should meet separately from management 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. The audit committee should not only focus on what the auditors are doing to detect fraud, but more importantly 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[15] 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.[16] The audit committee should insist on openness and honesty with the external auditors. The external auditors should also have commitment and cooperation from the audit committee. This includes open and candid dialogue between audit committee members and the external auditors regarding the audit 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 the organization has established to mitigate these risks.

The audit committee should also seek the advice of legal counsel whenever dealing with issues of allegations of fraud. Fraud allegations should be taken seriously since there may be a legal obligation to investigate and/or report them.

In addition, since reputation risk resulting from fraudulent behavior often has a severe impact on shareholder value, the audit committee should provide specific consideration and oversight of this exposure when reviewing the work of management and internal auditors, and ask them to be alert for and report such exposure as they carry out their duties.

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 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.

---

[15] 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.

[16] Internationally, refer to International Standards on Auditing (ISA) No. 240, *The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements*. In the United States, refer to Statement of Auditing Standards (SAS) No. 99 (AU sec 316), Consideration of Fraud in a Financial Statement Audit; SAS No. 1 (AU sec 1), Codification of Auditing Standards and Procedures; PCAOB AS5; and Section 10A of the Securities Exchange Act of 1934. In Canada, refer to *CICA Handbook – Assurance* Section 5135, The Auditor's Responsibility to Consider Fraud. One may also refer to the International Organisation of Supreme Audit Institutions (INTOSAI), the International Federation of Accountants (IFAC) International Auditing and Assurance Standards Board (IAASB), and the Association of Chartered Certified Accountants (ACCA).

- Implementing adequate internal controls — including documenting fraud risk management policies and procedures and evaluating their effectiveness — 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.

Whenever the external auditor has determined that there is evidence that fraud may exist, the external auditor's professional standards require that the matter should be brought to the attention of an appropriate level of management in a timely manner. If the external auditor suspects fraud involving management, the external auditor must report these suspicions to those charged with governance (e.g., the audit committee).

In many organizations, one executive-level member of management is appointed to be responsible for fraud risk management and to report to the board periodically. This executive, a chief ethics officer for instance, is responsible for entity-level controls that establish the tone at the top and corporate culture. These expectations are often documented in the organization's values or principles, code of conduct, and related policies; demonstrated through executive communications and behaviors; and included in training programs. The person appointed should be familiar with the organization's fraud risks and process-level controls, and is often responsible for the design and implementation of the processes used to ensure compliance, reporting, and investigation of alleged violations.

Staff

Strong controls against fraud are the responsibility of everyone in the organization. The importance of internal controls in fraud risk management is not a new concept. In 1992, after more than three years of collaboration between corporate leaders, legislators, regulators, auditors, academics, and many others, COSO presented a common definition of internal controls and provided a framework against which organizations could assess and improve their internal control systems. COSO identified five components in its landmark *Internal Control–Integrated Framework* — control environment, risk assessment, control activities, information and communication, and monitoring — that may serve as the premise for the design of controls. The elements are deeply intertwined and overlapping in their nature, providing a natural interactive process to promote the type of environment in which fraud simply will not be tolerated at any level.[17]

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 (e.g. the fraud policy, code of conduct, and whistleblower policy), as well as other operational policies and procedures, such as procurement manuals.

[17] Appendix I suggests control activities aligned with each COSO component.

- 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

The IIA's Definition of Internal Auditing states, "Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." In relation to fraud, this means that internal auditing provides assurance to the board and to management that the controls they have in place are appropriate given the organization's risk appetite.

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 with regard to management override risks[18].

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. They should interview and communicate regularly with those conducting the organization's risk assessments, as well as others in key positions throughout the organization, to help them ensure that all fraud risks have been considered appropriately. When performing engagements, internal auditors should spend 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 and 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.[19]

The importance an organization attaches to its internal audit function is an indication of the organization's commitment to effective internal control. The internal audit charter, which is approved by the board or designated committee, should include internal auditing's roles and responsibilities related to fraud. Specific internal audit roles in relation to fraud risk management could include initial or full investigation of suspected fraud, root cause analysis and control improvement recommendations, monitoring of a reporting/whistleblower hotline, and providing ethics training sessions.[20] If assigned such duties, internal auditing has a responsibility to obtain sufficient skills and competencies, such as knowledge of fraud schemes, investigation techniques, and laws. Effective internal audit functions are adequately funded, staffed, and trained, with appropriate specialized skills given the nature, size, and complexity of the organization and its operating environment. Internal auditing should be independent (have independent authority and reporting relationships), have adequate access to the audit committee, and adhere to professional standards.

---

[18] Refer to the AICPA's *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention* publication.

[19] Refer to IIA Practice Advisory 2130-1: Role of the Internal Audit Activity and Internal Auditor in the Ethical Culture of an Organization.

[20] For additional information, refer to IIA Practice Advisories 1210-A2-1: Auditor's Responsibilities Relating to Fraud Risk Assessment, Prevention, and Detection; and 1210-A2-2: Auditor's Responsibilities Relating to Fraud Investigation, Reporting, Resolution, and Communication; as well as the IIA–UK and Ireland Fraud Position Statement.

FRAUD RISK MANAGEMENT PROGRAM COMPONENTS

Most organizations have written policies and procedures to manage fraud risks, such as codes of conduct, expense account procedures, and incident investigation standards. They usually have some activities that management has implemented to assess risks, ensure compliance, identify and investigate violations, measure and report the organization's performance to appropriate stakeholders, and communicate expectations. However, few have developed a concise summary of these documents and activities to help them communicate and evaluate their processes. We refer to the aggregate of these as the fraud risk management program ("program"), even if the organization has not formally designated it as such.

It is management's prerogative, with oversight from the board, to determine the type and format of documentation it wishes to adopt for its program. Suggested formats include:

- A single comprehensive and complete document that addresses all aspects of fraud risk management (i.e., a fraud control policy[21]).
- A brief strategy outline emphasizing the attributes of fraud control, but leaving the design of specific policies and procedures to those responsible for business functions within the organization.
- An outline, within a control framework, referencing relevant policies, procedures, plans, programs, reports, and responsible positions, developed by the organization's head office, divisions, or subsidiaries.[22]

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:

Commitment

The board and senior management should communicate their commitment to fraud risk management. One method would be to embed this commitment in the organization's values or principles and code of conduct. Another method is issuing a short document (e.g., letter) made available to all employees, vendors, and customers. This summary document should stress the importance of fraud risk mitigation, acknowledge the organization's vulnerability to fraud, and establish the responsibility for each person within the organization to support fraud risk management. The letter should be endorsed or authored by a senior executive or board member, provided to employees as part of their orientation process, and reissued periodically. The letter could serve as the foundation for, and may be the executive summary of, a fraud control policy.

Fraud Awareness

An ongoing awareness program is a key enabler to convey fraud risk management expectations, as well as an effective preventive control. Awareness of fraud and misconduct schemes is developed through periodic

[21] For examples of fraud control policies, see Appendices B and C.

[22] Some organizations centralize fraud risk management information under the chief ethics officer or within a framework used by internal auditing or the chief financial officer. Others may have this information spread out across the organization — for example, investigation standards and files in legal, hiring and training information in human resources, hotline information in internal auditing, risk assessment in the enterprise risk management group — and will need to compile it to do an effective evaluation and to enable concise reporting to the board.

assessment, training, and frequent communication. An organization's fraud risk management program will assist the organization with fraud awareness. Documentation to support fraud awareness should define and describe fraud and fraud risks.[23] It should also provide examples of the types of fraud that could occur and identify potential perpetrators of fraud.

When designing fraud awareness programs, management should consider who should attend, frequency and length, cultural sensitivities, guidance on how to solve ethical dilemmas, and delivery methods. Management should also consider the training needs of the board or board committee members.

Affirmation Process

An organization should determine whether there are any legal issues involved with having an affirmation process, which is the requirement for directors, employees, and contractors to acknowledge they have read, understood, and complied with the code of conduct, a fraud control policy, and other such documentation to support the organization's fraud risk management program. There is a fraud risk to the organization of not having an affirmation process. This should be acknowledged and accepted at or above a senior management level.

The affirmation process may be handled electronically or via manual signature. Organizations implementing best practice often also require personnel to acknowledge that they are not aware of anyone who is in violation of the policies. Management should establish consequences for refusal to sign-off and apply such action consistently.

Some organizations include terms in their contracts that require service providers to agree to abide by the organization's code of conduct, a global standard, or the like, which may also prevent fraud. Others require senior management to sign a code of conduct specific to employees at higher levels of the organization and require service providers to sign separate agreements on specific topics, such as confidentiality or use of company technologies.

Conflict Disclosure

A process should be implemented for directors, employees, and contractors to internally self-disclose potential or actual conflicts of interest. Once conflicts are internally disclosed, there are several decision paths:

- Management may assert that there is in fact, a conflict and require the individual to terminate the activity or leave the organization.
- Management may accept the internal disclosure and determine that there is no conflict of interest in the situation described.
- Management may decide that there is a potential for conflict of interest and may impose certain constraints on the individual to manage the identified risk and to ensure there is no opportunity for a conflict to arise.

The disclosure of a potential conflict of interest and management's decision[24] should be documented and disclosed to legal counsel. Any constraints placed on the situation need to be monitored. For example, a buyer who has

---

[23] Refer to Section 2 (Fraud Risk Assessment) for a more detailed discussion of fraud risks and risk assessments.

[24] Conflict of interest policy provision waivers for executive officers of New York Stock Exchange-listed companies can only be granted by the board of directors or a committee thereof, and such waivers have to be disclosed to shareholders promptly. Waivers for executive officers of NASDAQ-listed companies can only be granted by independent board members, and such waivers need to be disclosed.

recently been hired in the purchasing department is responsible for all purchases in Division A. His brother has a local hardware store that supplies product to Division A. The buyer discloses the potential conflict of interest and is told that transactions with the hardware store are permitted, as long as the department supervisor monitors a monthly report of all activity with the hardware store to ensure the activity and price levels are reasonable and competitive. When the buyer is promoted or transferred, the constraints may be removed or altered.

Other disclosure processes may also exist, such as insider trading disclosures. Those processes that mitigate potential fraud risk should be linked to the fraud risk management program. Organizations should evaluate the legal requirements and/or business benefits of disclosing their code of conduct, fraud control policy, or related statements to the public.

Fraud Risk Assessment[25]

The foundations of an effective fraud risk management program are rooted in a risk assessment, overseen by the board, which identifies where fraud may occur within the organization. A fraud risk assessment should be performed on a systematic and recurring basis, involve appropriate personnel, consider relevant fraud schemes and scenarios, and mapping those fraud schemes and scenarios to mitigating controls. The existence of a fraud risk assessment and the fact that management is articulating its existence may even deter would-be fraud perpetrators.

The system of internal controls in an organization is designed to address inherent business risks. The business risks are identified in the enterprise risk assessment protocol, and the controls associated with each risk are noted. COSO's *Enterprise Risk Management–Integrated Framework* describes the essential ERM components, principles, and concepts for all organizations, regardless of size.

Reporting Procedures and Whistleblower Protection

Documentation should not only articulate the organization's zero tolerance[26] for fraud, it should also establish the expectation that suspected fraud must be reported immediately and provide the means to do so. The channels to report suspected fraud issues should be clearly defined and communicated. These may be the same or different from channels for reporting other code of conduct violations.

Considering that people commit fraud and that people are an organization's best asset in preventing, detecting, and deterring fraud, an organization should consider promoting available fraud reporting resources that individuals may access, such as a fraud or ethics page on the organization's Web site, an ombudsman, or a whistleblower hotline. To encourage timely reporting of suspected issues, the organization should communicate the protections afforded to the individual reporting the issue — often referred to as whistleblower protection. In some countries, securities regulations require organizations to have whistleblower protection.

---

[25] For more information on fraud risk assessments, refer to Section 2: Fraud Risk Assessment.

[26] ALARM (The National Forum for Risk Management in the Public Sector (UK)) lists a culture of zero tolerance as one of five essential governance strategies to manage fraud risk. Other strategies include an embedded strategic approach to risk management, a sound counter-fraud and corruption framework, strong systems of internal control, and close working relationships with partners regarding fraud risk management activities.

Investigation Process[27]

Organizations should require that an investigation process be in place. Once an issue is suspected and reported, an investigation process will follow. The board and management should have a documented protocol for this process, including consideration of who should conduct the investigation — whether it be internal personnel or hiring experts in this field — rules of evidence, chains of custody, reporting mechanisms to those charged with governance, regulatory requirements, and legal actions. Organizations should also consider whether to require all employees, as a condition of employment, to cooperate fully with an investigation into any alleged or suspected fraud.

Corrective Action

As a deterrent, policies should reflect the consequences and processes for those who commit or condone fraudulent activity. These consequences may include termination of employment or of a contract and reporting to legal and regulatory authorities. The organization should articulate that it has the right to institute civil or criminal action against anyone who commits fraud.

When fraud does occur within the organization, policies should reflect the need to conduct a postmortem to identify the control weakness that contributed to the fraudulent act. The postmortem should lead to a remediation of any identified control deficiencies. Internal auditors are important resources for this activity.

Process Evaluation and Improvement (Quality Assurance)

Documentation should describe whether, and/or how, management will periodically evaluate the effectiveness of the fraud risk management program and monitor changes. It may include the need for measurements and analysis of statistics, benchmarks, resources, and survey results. The results of this evaluation should be reported to appropriate oversight groups and be used by management to improve the fraud risk management program.

Continuous Monitoring

The fraud risk management program, including related documents, should be revised and reviewed based on the changing needs of the organization, recognizing that documentation is static, while organizations are dynamic. Fraud risk management program documentation should be updated on an ongoing basis to reflect current conditions and to reflect the organization's continuing commitment to the fraud risk management program.

SECTION 2: FRAUD RISK ASSESSMENT

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.

Regulators, professional standard-setters, and law enforcement authorities have emphasized the crucial role risk assessment plays in developing and maintaining effective fraud risk management programs and controls.[28]

[27] Refer to Section 5 (Investigation and Corrective Action) for more details on the investigation process and corrective action.

[28] Refer to June 2007 SEC Guidance to Management; PCAOB AS5; IIA Practice Advisory 1210-A2-1: Auditor's Responsibilities Relating to Fraud Risk Assessment, Prevention, and Detection; *COSO for Small Business:* Principle 10–Fraud Risk; SAS No. 99, Consideration of Fraud in A Financial Statement Audit; and ISA No. 240.

Organizations can identify and assess fraud risks in conjunction with an overall enterprise risk assessment or on a stand-alone basis.

Guidance for conducting a fraud risk assessment is provided in this section of the guide. Organizations can tailor this approach to meet their individual needs, complexities, and goals.

The foundation of an effective fraud risk management program should be seen as a component of a larger enterprise risk management (ERM) effort and is rooted in a risk assessment that identifies where fraud may occur and who the perpetrators might be. To this end, control activities should always consider both the fraud scheme and the individuals within and outside the organization who could be the perpetrators of each scheme. If the scheme is collusive[29], preventive controls should be augmented by detective controls, as collusion negates the control effectiveness of segregation of duties.

Fraud, by definition, entails intentional misconduct, designed to evade detection. As such, the fraud risk assessment team should engage in strategic reasoning to anticipate the behavior of a potential fraud perpetrator.[30] Strategic reasoning, which is also important in designing fraud detection procedures that a perpetrator may not expect, requires a skeptical mindset 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?
- What could a perpetrator do to conceal the fraud?

With this in mind, a fraud risk assessment generally includes three key elements:

- *Identify inherent fraud risk*[31] — Gather information to obtain the population of fraud risks that could apply to the organization. Included in this process is the explicit consideration of all types of fraud schemes and scenarios; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to the organization.

- *Assess likelihood and significance of inherent fraud risk* — Assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with staff, including business process owners.

- *Respond to reasonably likely and significant inherent and residual fraud risks* — Decide what the response should be to address the identified risks and perform a cost-benefit analysis of fraud risks over which the organization wants to implement controls or specific fraud detection procedures.

---

[29] A collusive scheme is one performed by two or more individuals working together.

[30] T. Jeffrey Wilks and M.F. Zimbelman, "Using Game Theory and Strategic Reasoning Concepts to Prevent and Detect Fraud," *Accounting Horizons*, Volume 18, No. 3 (September 2004).

[31] 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.

Organizations should apply a framework to document their fraud risk assessment. The framework below illustrates how the elements of fraud risk identification, assessment, and response are applied in a rational, structured approach. This example begins with a list of identified fraud risks and schemes, which are then assessed for relative likelihood and significance of occurrence. Next, the risks and schemes are mapped to the people and/or departments that may be impacted and to relevant controls, which are evaluated for design effectiveness and tested to validate operating effectiveness. Lastly, residual risks are identified, and a fraud risk response is developed.[32]

Identified Fraud Risks and Schemes	Likelihood	Significance	People and/or Department	Existing Anti-fraud Controls	Controls Effectiveness Assessment	Residual Risks	Fraud Risk Response
Financial reporting Revenue recognition - Backdating agreements - Channel stuffing - Inducing distributors to accept more product than necessary - Holding books open - Via recording detail transactions in a sub-ledger - Via recording top-side journal entries - Additional revenue risks Management estimates - Self insurance - Altering underlying detail claims and estimate data - Fraudulently changing underlying assumptions in estimation of liability - Allowance for bad debts - Altering underlying A/R aging to manipulate computation - Fraudulent input from sales persons or credit department on credit quality - Additional estimates Disclosures - Footnotes - Additional disclosures *Misappropriation of assets* Cash/check - Point of sale - Accounts receivable application process - Master vendor file controls override - Additional risks - Inventory - Theft by customers - Theft by employees - Other assets at risk *Corruption* - Bribery - Aiding and abetting *Other Risks*							

[32] Refer to Appendix D of this document for an example of the use of this framework.

THE RISK ASSESSMENT TEAM

A good risk assessment requires input from various sources. Before conducting a risk assessment, management should identify a risk assessment team. This team should include individuals from throughout the organization with different knowledge, skills, and perspectives and should include a combination of internal and external resources such as:

- Accounting/finance personnel, who are familiar with the financial reporting process and internal controls.
- Nonfinancial business unit and operations personnel, to leverage their knowledge of day-to-day operations, customer and vendor interactions, and general awareness of issues within the industry.
- Risk management personnel, to ensure that the fraud risk assessment process integrates with the organization's ERM program.
- Legal and compliance personnel, as the fraud risk assessment will identify risks that give rise to potential criminal, civil, and regulatory liability if the fraud or misconduct were to occur.
- Internal audit personnel, who will be familiar with the organization's internal controls and monitoring functions. In addition, internal auditors will be integral in developing and executing responses to significant risks that cannot be mitigated practically by preventive and detective controls.
- 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) should participate in the assessment, as they are ultimately accountable for the effectiveness of the organization's fraud risk management efforts.

FRAUD RISK IDENTIFICATION

Once assembled, the risk assessment team should go through 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 openness to ideas regarding potential risks and controls[33]. Brainstorming enables discussions of the incentives, pressures, and opportunities to commit fraud; risks of management override of controls; and the population of fraud risks relevant to the organization.[34] Other risks, such as regulatory and legal misconduct and reputation risk, as well as the impact of IT on fraud risks also should be considered in the fraud risk identification process.

The organization's fraud risk identification information should be shared with the board or audit committee and comments should be solicited. The board also should assess the implications of its own processes with respect to its contribution to fraud risk, including incentive pressures.

[33] Sources of information about good brainstorming practices include (a) Mark S. Beasley and Gregory Jenkins, "A Primer for Brainstorming Fraud Risks," Journal of Accountancy, December 2003, and (b) Michael J. Ramos, "Brainstorming Prior to the Audit," in *Fraud Detection in a GAAS Audit: Revised Edition*, Chapter 2: "Considering Fraud in a Financial Statement Audit."

[34] Refer to Appendix E: Fraud Risk Exposures of this document for a list of potential fraud risk which could be used in brainstorming.

Incentives, Pressures, and Opportunities

Motives for committing fraud are numerous and diverse. One executive may believe that the organization's business strategy will ultimately be successful, but interim negative results need to be concealed to give the strategy time. Another needs just a few more pennies per share of income to qualify for a bonus or to meet analysts' estimates. The third executive purposefully understates income to save for a rainy day.

The fraud risk identification process should include an assessment of the incentives, pressures, and opportunities to commit fraud. Incentive programs should be evaluated — by the board for senior management and by management for others — as to how they may affect employees' behavior when conducting business or applying professional judgment (e.g., estimating bad debt allowances or revenue recognition). Financial incentives and the metrics on which they are based can provide a map to where fraud is most likely to occur. There may also be nonfinancial incentives, such as when an employee records a fictitious transaction so he or she does not have to explain an otherwise unplanned variance. Even maintaining the status quo is sometimes a powerful enough incentive for personnel to commit fraud.

Also important, and often harder to quantify, are the pressures on individuals to achieve performance or other targets. Some organizations are transparent, setting specific targets and metrics on which personnel will be measured. Other organizations are more indirect and subtle, relying on corporate culture to influence behavior. Individuals may not have any incremental monetary incentive to fraudulently adjust a transaction, but there may be ample pressure — real or perceived — on an employee to act fraudulently.

Meanwhile, 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 difficult to detect because management can often override the controls. Such opportunities are why appropriate monitoring of senior management by a strong board and audit committee, supported by internal auditing, is critical to fraud risk management.

Risk of Management's Override of Controls

As part of the risk identification process, it is important to consider the potential for management override of controls established to prevent or detect fraud. Personnel within the organization generally know the controls and standard operating procedures that are in place to prevent fraud. It is reasonable to assume that individuals who are intent on committing fraud will use their knowledge of the organization's controls to do it in a manner that will 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 just submit false invoices for payment. Hence, it is also important to keep the risk of management's override of controls in mind when evaluating the effectiveness of controls; an anti-fraud control is not effective if it can be overridden easily.

Population of Fraud Risks

The fraud risk identification process requires an understanding of the universe of fraud risks and the subset of risks specific to the organization. This may involve obtaining information from external sources such as industry news; criminal, civil, and regulatory complaints and settlements; and organizations such as The IIA, AICPA, ACFE, and CICA.

This also involves understanding the organization's business processes and gathering information about potential fraud from internal sources by interviewing personnel and brainstorming with them, reviewing complaints from the whistleblower hotline, and performing analytical procedures.

Various taxonomies are available to organize fraud risks. Appendix H displays the Foundation Principles issued by the Open Compliance and Ethics Group (OCEG) that relate to fraud risk identification. The ACFE, on the other hand, classifies occupational fraud risks into three general categories: fraudulent statements, misappropriation of assets, and corruption[35]. Using the ACFE's categories as a starting point, a more detailed breakout can be developed to produce an organization-specific fraud risk assessment. For example, potential fraud risks to consider in the ACFE's three general categories include:

1) Intentional manipulation of financial statements, which can lead to:
    a) Inappropriately reported revenues.
    b) Inappropriately reported expenses.
    c) Inappropriately reflected balance sheet amounts, including reserves.
    d) Inappropriately improved and/or masked disclosures.
    e) Concealing misappropriation of assets.
    f) Concealing unauthorized receipts and expenditures.
    g) Concealing unauthorized acquisition, disposition, and use of assets.

2) Misappropriation of:
    a) Tangible assets by:
        i) Employees.
        ii) Customers.
        iii) Vendors.
        iv) Former employees and others outside the organization.
    b) Intangible assets.
    c) Proprietary business opportunities.

3) Corruption including:
    a) Bribery and gratuities to:
        i) Companies.
        ii) Private individuals.
        iii) Public officials.
    b) Receipt of bribes, kickbacks, and gratuities.
    c) Aiding and abetting fraud by other parties (e.g., customers, vendors).

Fraudulent Financial Reporting

Each of the three categories outlined by the ACFE includes at least one scheme of how the fraud could occur. For instance, acceleration of revenue recognition can be achieved via numerous schemes, including backdating agreements, recognizing revenue on product not shipped by period end, or channel stuffing. Some fraudulent

[35] The ACFE's Report to the Nation on Occupational Fraud and Abuse.

financial reporting schemes are common across all organizations (e.g., setting aside unsupported reserves for use in future periods and fraudulent top-side entries); other schemes are more industry-specific (e.g., backdating agreements at software companies or channel stuffing for organizations that sell via distributors). Each scheme that could be relevant to the organization should be considered in the assessment.

Organizations can use the framework in Appendix D to identify specific areas of greatest risk and 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 assessment should consider 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?
- What are the incentives and pressures present in the organization?
- Are revenues recorded systematically or manually?
- Are there any revenue recognition fraud risks specific to the organization's industry?

For significant marketplace disclosures (e.g., loan delinquency percentages) consider the following questions:

- What controls are in place to monitor internal gathering and reporting of these disclosures?
- Is there oversight from someone whose compensation is not directly affected by his or her performance?
- 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?

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

Another consideration involves fraud where the objective is not to improve the organization's financial statements, but to cover up a hole left by the misappropriation or misuse of assets. In this case, the fraud also includes fraudulent financial reporting.

Misappropriation of Assets

An organization's assets, both tangible (e.g., cash or inventory) and intangible (e.g., proprietary or confidential product, or customer information), can be misappropriated by employees, customers, or vendors. The organization should ensure that controls are in place to protect such assets. Considerations to be made 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 schemes include misappropriation by:

- Employees.
  - Creation of, and payments to, fictitious vendors.
  - Payment of inflated or fictitious invoices.

    - Invoices for goods not received or services not performed.
    - Theft of inventory or use of business assets for personal gain.
    - False or inflated expense claims.
    - Theft or use of customer lists and proprietary information.
- Employees in collusion with vendors, customers, or third parties.
    - Payment of inflated or fictitious invoices.
    - Issuance of inflated or fictitious credit notes.
    - Invoices for goods not received or services not performed.
    - Preferred pricing or delivery.
    - Contract bid rigging.
    - Theft or use of customer lists and proprietary information.
- Vendors.
    - Inflated or fictitious invoices.
    - Short shipments or substitution of lower quality goods.
    - Invoices for goods not received or services not preformed.
- Customers.
    - False claims for damaged or returned goods or short shipments.

Protecting against these risks requires not only physical safeguarding controls, but also periodic detective controls such as physical counts of inventory with reconciliations to the general ledger. Remember, a smart perpetrator may be thinking about such controls and design the fraud to circumvent or be concealed from those controls. Those conducting the risk assessment should keep this in mind when deliberating misappropriation of asset schemes and their impact to the organization.

Corruption

Corruption is operationally defined as the misuse of entrusted power for private gain. In the United States, 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. There are similar anti-corruption laws in other countries as well as guidelines established by the United Nations Convention Against Corruption, to which more than 100 countries are signatories.

Organizations that have operations outside their home countries need to consider other relevant anti-corruption laws when establishing a fraud risk management program. Transparency International, a multinational organization focused on anti-corruption and transparency in business and government, issues an annual Corruption Perception Index, which ranks countries on their perceived levels of corruption. The Corruption Perception Index can assist organizations in prioritizing their anti-corruption efforts in areas of the world at greatest risk. It must be remembered, of course, that corruption can also occur in an organization's home country.

A common form of corruption is aiding and abetting. Law enforcement authorities worldwide have prosecuted numerous cases where organizations were not misstating their financial statements, but were knowingly structuring transactions or making representations that enabled other organizations to fraudulently misstate their financial statements. A thorough risk assessment will consider the risk that someone may be engaging in such behavior as well as other types of corruption that may be applicable to the organization.

Information Technology and Fraud Risk

Organizations rely on IT to conduct business, communicate, and process financial information. A poorly designed or inadequately controlled IT environment can expose an organization to fraud. Today's 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. IT is an important component of any risk assessment, especially when considering fraud risks. IT risks include threats to data integrity, threats from hackers to system security, and theft of financial and sensitive business information. Whether in the form of hacking, economic espionage, Web defacement, sabotage of data, viruses, or unauthorized access to data, IT fraud risks can affect everyone. In fact, IT can be used by people intent on committing fraud in any of the three occupational fraud risk areas defined by the ACFE.

Examples of those risks by area 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. IT personnel may be able to access restricted data or adjust records fraudulently.

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, more and more valuable assets of organizations are intangibles such as 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.

Corruption

- *Misuse of customer data* — Personnel within or outside the organization can obtain employee or customer data and use such information to obtain credit or for other fraudulent purposes.

Keep in mind, cyber fraudsters do not even have to leave their homes to commit fraud, as they can route communications through local phone companies, long-distance carriers, Internet service providers, and wireless and satellite networks. They may go through computers located in several countries before attacking targeted systems around the globe. What is important is that any information — not just financial — 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, an organization should know its vulnerabilities and be able to mitigate risk in a cost-effective manner. Therefore, IT risk should be incorporated into an organization's overall fraud risk assessment.

OTHER RISKS

Regulatory and Legal Misconduct

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 should be considered in the risk assessment process.

Reputation Risk

Reputation risk is evaluated differently by different individuals, 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, 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. Because the board is responsible for the longevity of the organization and has responsibilities to multiple stakeholders, it should 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.

ASSESSMENT OF THE LIKELIHOOD AND SIGNIFICANCE OF IDENTIFIED INHERENT FRAUD RISKS

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 impact on every organization. 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 business on an inherent basis, or without consideration of known controls. By taking this approach, management will be better able to consider all relevant fraud risks and design controls to address the risks. After mapping fraud risks to relevant controls, certain residual risks will remain, including the risk of management's override of established controls. Management must evaluate the potential significance of those residual risks and decide on the nature and extent of the fraud preventive and detective controls and procedures to address such risks.

Likelihood — Management's assessment of the likelihood of a fraud risk occurring is informed by instances of that particular fraud occurring in the past at the organization, the prevalence of the fraud risk in the organization's industry, and other factors, including the number of individual transactions, the complexity of the risk, and the number of people involved in reviewing or approving the process. Organizations can categorize the likelihood of potential frauds occurring in as many buckets as deemed reasonable, but three categories are generally adequate: remote, reasonably possible, and probable.

Significance — Management's assessment of the significance of a fraud risk should include not only financial statement and monetary significance, but also significance to an organization's operations, brand value, and reputation, as well as criminal, civil, and regulatory liability. For example, two different organizations may have similar amounts of expenses charged via employee expense reports, but one organization 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 relationships. Organizations can categorize the significance of potential frauds in as many buckets as deemed reasonable, but three categories are generally adequate: inconsequential, more than inconsequential, and material.

People/department — As part of the risk assessment process, the organization will have evaluated the incentives and pressures on individuals and departments and should use the information gained in that process to assess which individuals or departments are most likely to have incentive to commit a fraudulent act, and, if so, via what means. This information can be summarized into the fraud risk assessment grid and can help the organization design appropriate risk responses, if necessary.

RESPONSE TO RESIDUAL FRAUD RISKS

Risk tolerance varies from organization to organization. At the highest level, the board sets the organization's risk tolerance level, taking into consideration its responsibilities to all shareholders, capital providers, and 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. Many organizations will state that there is a "zero tolerance" policy with respect to fraud. However, there may be certain fraud risks that an organization considers too expensive and time-consuming to address via controls. Consequently, the organization may decide not to put controls in place to address such risks. If a fraud is discovered, zero tolerance for fraud will be applied.

An organization's risk tolerance level provides management support on how to respond to fraud risk. Fraud risks can be 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, or designing internal audit procedures to address specific fraud risks. The board should ensure management has implemented the right level of controls based on the risk tolerance it has established for the organization. In effect, one should look at an organization's financial statements and operations and ask "What can be wrong in this picture?", and then design appropriate controls. The key is to be selective and efficient. There are probably thousands of potential controls that could be put in place. The goal is a targeted and structured approach — not an unstructured or haphazard approach — and efficient controls that deliver the most benefit for the cost of resources. The overall objective is to have the benefit of controls exceed their cost.

In addressing fraud risks, one should be careful to ensure that anti-fraud controls are operating effectively and have been designed to include appropriate steps to deal with the relevant risks. Where an internal control might be executed with limited skepticism (e.g., agreeing an accrual balance to underlying support) an anti-fraud control would include an evaluation of the underlying support for consistency in application from prior periods and for potential inappropriate bias. Therefore, anti-fraud controls should be designed appropriately and executed by competent and objective individuals. Management's documentation of anti-fraud controls should include 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.

SECTION 3: FRAUD PREVENTION

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

Despite the best efforts of those responsible for preventing fraud, one inevitable reality remains: "fraud happens." Because fraud and misconduct can occur at various levels in any organization, it is essential that appropriate preventive and detective techniques are in place. Although fraud prevention and detection are related concepts, they are not the same. While prevention encompasses policies, procedures, training, and communication, detection involves activities and programs designed to identify fraud or misconduct that is occurring or has occurred. Although preventive measures cannot ensure that fraud will not be committed, they are the first line of defense in minimizing fraud risk. This section of the guide will cover preventive techniques. Detective techniques will be covered in Section 4.

One key to prevention is making personnel throughout the organization aware of the fraud risk management program, including the types of fraud and misconduct that may occur. This awareness should enforce the notion that all of the techniques established in the program are real and will be enforced. The ongoing communication efforts could provide information on the potential disciplinary, criminal, and civil actions that the organization could take against the individual.

With this in mind, prevention and deterrence are interrelated concepts. If effective preventive controls are in place, working, and well-known to potential fraud perpetrators, they serve as strong deterrents to those who might otherwise be tempted to commit fraud. Fear of getting caught is always a strong deterrent. Effective preventive controls are, therefore, strong deterrence controls.

The system of internal controls in an organization is designed to address inherent business risks. The business risks are identified in the enterprise risk assessment protocol, and the controls associated with each risk are noted. COSO's *Enterprise Risk Management–Integrated Framework* describes the essential ERM components, principles, and concepts for all organizations, regardless of size.

Establishing internal controls may not address all of an organization's fraud risks. Fraud risks, although a form of business risk, necessitate specific controls to mitigate them, which makes an organization's fraud risk assessment process essential to fraud prevention. In addition to implementing fraud preventive controls, it is important that the organization assess and continuously monitor their operational effectiveness to help prevent fraud from occurring.

FRAUD PREVENTIVE CONTROLS

Prevention is the most proactive fraud-fighting measure. The design and implementation of control activities should be a coordinated effort spearheaded by management with an assembled cast of employees. Collectively, this cross section of the organization should be able to address all of the identified risks, design and implement the control activities, and ensure that the techniques used are adequate to prevent fraud from occurring in accordance with the organization's risk tolerance.

The ongoing success of any fraud prevention program depends on its continuous communication and reinforcement. Stressing the existence of a fraud prevention program through a wide variety of media — posters on bulletin boards, flyers 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.

Among the many elements in fraud prevention are HR procedures, authority limits, and transaction level procedures.

Human Resources Procedures

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

Performing Background Investigations

A key business and fraud risk in any organization lies in the people hired to operate the business and promoted into positions of trust and authority. For that reason, it is important to know employees in order to evaluate their credentials and competence, match skills to the job requirements, and be aware of any issues of personal integrity that may impact 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 or in follow-up with references provided. It is possible to find false or embellished information or undisclosed history and reputation that may represent increased, and possibly unacceptable, risk.

While the organization should establish 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 only be possible upon receiving the individual's consent. Legal counsel should be sought to advise on what background information can and cannot be obtained and the appropriate procedures to follow.

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

Anti-fraud Training

An organization can hire or promote competent individuals who, having undergone appropriate background checks, represent a low fraud risk. It is possible that such individuals have a comprehensive understanding of what fraud is and what its red flags are, and an appreciation of its potential to devastate an organization. There should not, however, be any exemption from receiving an initial orientation and ongoing education on the fraud risk management program in place, regardless of the individual's position in the organization. Such education serves to establish and reinforce the tone from the top regarding the individual's responsibility and the process to deal with suspected fraud.

An organization's HR group is often 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. The effectiveness of this training is dependent on mandatory attendance with periodic updates and refresher sessions.

Evaluating Performance and Compensation Programs
HR managers should be involved in both the 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 of competence and reward for positive performance and success. Regular and robust assessment of employee performance with timely and constructive feedback goes a long way to preventing potential problems. Employees who are not recognized for what they do and what they have accomplished, especially those who may have been bypassed for promotion, may feel their inappropriate and fraudulent conduct is justified.

Reward can also be reflected in compensation. By conducting compensation surveys and local market analysis, HR can determine whether senior management and employees are compensated appropriately and therefore driving desired behavior by striking a balance between fixed and variable compensation. 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.

Conducting Exit Interviews
A policy of conducting exit interviews of terminated employees or those who have resigned can help in both prevention and detection efforts. These interviews may help HR managers determine whether there are issues regarding management's integrity or information regarding conditions conducive to fraud. HR should also review the content and information contained in resignation letters as they may contain information regarding possible fraud and misconduct existing within the organization.

Authority 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.

An organization may establish authoritative approval levels across the enterprise to serve as an entity-level control. On the other hand, individuals working within a specific function may be assigned only limited IT access as a process-level control. These types of controls, supported by an appropriate segregation of duties, assist in the first line of defense in fraud prevention.

Transaction-level Procedures

Reviews of third-party and related-party transactions can also help prevent fraud. Because fraud schemes often involve the use of third-party entities/individuals, organizations need thorough measures at the front-end that

will prevent the back-end activities. False vendors or employees are two of the more obvious and noted schemes in this arena.

Preventive measures are especially needed for related-party transactions that can be controlled by board members or by employees of authority with an interest in an outside entity with which the organization may conduct business. Such individuals may mandate transactions that ultimately benefit them at the expense of the organization.

DOCUMENTATION OF FRAUD PREVENTION TECHNIQUES

An organization should formally document the techniques developed and implemented to prevent fraud. This includes documenting processes used to monitor the performance of fraud preventive controls or to indicate when such controls are ineffective. Testing procedures conducted to ensure adequate operation of fraud preventive controls and the test results should also be thoroughly documented.

Paramount to this documentation is a detailed description of the elements of the organization's fraud prevention techniques, with emphasis placed on the roles and responsibilities of all parties involved.

ASSESSING THE ORGANIZATION'S FRAUD PREVENTION

Organizations just beginning to assess their fraud risk management program, as well as organizations striving to improve their fraud risk management program, should conduct overall assessments of their fraud prevention techniques. The Fraud Prevention Scorecard in Appendix F can be used to assess how comprehensive the organization's preventive controls are and how well they are working. Organizations should periodically reassess their fraud prevention techniques to ensure that progress is being made to get to an "all-green" fraud prevention status and that no elements of fraud prevention are deteriorating. Organizations with strong commitments to fraud prevention may also wish to engage independent outside experts to assess their fraud prevention techniques.

CONTINUOUS MONITORING OF FRAUD PREVENTIVE CONTROLS

The organization's plan, approach, and scope of monitoring its fraud prevention techniques should be documented and updated as necessary. With all of the parties involved in the risk assessment process and the subsequent design of the control activities, it is difficult to require that fraud prevention be monitored regularly by an independent entity. But reviews should be conducted separately from any routine or planned audits and should be designed to assure management of the effectiveness of the organization's fraud prevention.

Before each program review, issues such as significant changes in the organization and their associated risks, changes in personnel responsible for implementing the activities, and the results of previous assessments will determine if the scope of the current examination needs to be altered. Each evaluation should include evidence that management is actively retaining responsibility for oversight of the fraud risk management program, that timely and sufficient corrective measures have been taken with respect to any previously noted control deficiencies or weaknesses, and that the plan for monitoring the program continues to be adequate for ensuring the program's ongoing success.

SECTION 4: FRAUD DETECTION

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

Having effective detective controls in place and visible is one of the strongest deterrents to fraudulent behavior. Used in tandem with preventive controls, detective controls enhance a fraud risk management program's effectiveness by providing evidence that preventive controls are working as intended and identifying fraud that occurs. Although detective controls may provide evidence that fraud is occurring or has occurred, they are not intended to prevent fraud.

In some cases, the types of detective controls implemented may depend on the fraud risks identified for an organization. For example, if an organization operates in countries that are identified as having high risks for corruption, it may implement detective controls to identify possible violations of the FCPA, such as a recurring review of expense reports or consulting fees. Similarly, if an organization has a high frequency of subjective estimates, it may implement detective controls related to regular internal audit review of such activity. Overall, additional detection controls may be necessary based on the fraud risks identified for the organization. As with fraud prevention, it is important that the organization assess and continuously monitor its fraud detection techniques to help detect fraud that is occurring or has occurred.

FRAUD DETECTIVE CONTROLS

Organizations can never eliminate the risk of fraud entirely. There are always people who are motivated to commit fraud, and an opportunity can arise for someone in any organization to override a control or collude with others to do so. Therefore, detection techniques should be flexible, adaptable, and continuously changing to meet the various changes in risk.

While preventive measures are apparent and readily identifiable by employees, third parties, and others, detective controls are clandestine in nature. This means they operate in a background that is not evident in the everyday business environment. Such techniques will usually:

- Occur in the ordinary course of business.
- Draw on external information to corroborate internally generated information.
- Formally 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 eliminate all fraud risk. An organization may choose to design its controls to detect, rather than prevent, certain fraud risks, as approved by the board. If the estimated costs of designing, implementing, and monitoring the controls against fraud — such as tools, personnel, or training — exceeds the estimated impact of the risk, they may not be cost-effective to implement. For example, a property and casualty insurance company may set threshold limits on the total of losses paid plus those reserved on large policies to identify that fraud may be occurring, rather than relying solely on the identification of fraudulent individual claims. Important detection methods include an anonymous reporting mechanism

(whistleblower hotline), process controls, and proactive fraud detection procedures specifically designed to identify fraudulent activity.

Whistleblower Hotlines

The use of a whistleblower hotline[36], which has markedly increased among SEC registrants since it was mandated by the U.S. Sarbanes-Oxley Act of 2002, is one of the more effective measures organizations can implement as part of their fraud risk assessment program. Various surveys[37] indicate that anonymous tips received through hotlines or by other methods are the most likely means of detecting fraud. In addition, knowledge that an employee hotline is in place can help prevent fraud because individuals may fear that a fraud will be discovered and reported.

Marketing the existence of a hotline to increase awareness, making it easy to use, and promoting the timely handling of all reported issues are strong preventive measures that should supplement the detective control of hotlines. The hotline should be promoted with educational materials provided to shareholders, employees, customers, and vendors, all of whom can provide valuable information from a variety of reliable sources. Hotlines ideally support a multilingual capability and provide access to a trained interviewer 24 hours a day, 365 days a year.

Provision for anonymity to any individual who willingly comes forward to report a suspicion of fraud is a key to encouraging such reporting and should be a component of the organization's policy. The most effective whistleblower hotlines preserve the confidentiality of callers and provide assurance to employees that they will not be retaliated against for reporting their suspicions of wrongdoing including wrongdoing by their superiors. Another key is demonstrating that their reporting will result in appropriate and timely action being taken. To preserve the integrity of the whistleblower process, it must also provide a means of reporting suspected fraud that involves senior management, possibly reporting directly to the audit committee.

A single case management system should be used to log all calls and their follow-up to facilitate management of the resolution process, testing by internal auditors, and oversight by the board and/or the audit committee[38] as the board's designee. The board should approve protocols to ensure reported fraud-related issues are disseminated timely to appropriate parties, such as the ethics/compliance team, HR, the board and/or the audit committee, legal, and security. Distributing reports to these parties of occurrences in their respective areas of responsibility ensures that no single person or functional area controls this highly sensitive information and increases accountability. Charged with the responsibility for having documented procedures for receiving, retaining, and investigating complaints or tips alleging the possibility of misconduct or possible fraud, many audit committees have turned to independent service providers to operate hotlines and notify the organization of any reported accusations.

An effective hotline program should analyze the data received and compare results to norms for similar organizations. Ongoing analysis allows an organization to reshape its fraud risk management program to address evolving risks. The whistleblower process should be independently evaluated periodically for effectiveness, including compliance with established protocols.

---

[36] Whistleblower hotlines may not be legal or ethical, or may be subject to restrictions in some countries outside the United States. As such, multinational organizations may not be able to implement hotlines on a worldwide basis.

[37] The ACFE Occupational Fraud and Abuse Survey and the KPMG Fraud Survey are examples.

[38] The United Kingdom (UK) report, "Audit Committees Combined Code Guidance," by Sir Robert Smith, suggests that audit committees should review whistleblowing arrangements regarding the appropriate and independent investigations and follow-up action.

Process Controls

Process controls specifically designed to detect fraudulent activity, as well as errors, include reconciliations, independent reviews, physical inspections/counts, analyses, and audits. A lack of, or weakness in, preventive controls increases the risk of fraud and places a greater burden on detective controls. The more significant the fraud risk, the more sensitive to occurrence (e.g., use of thresholds, performance frequency, and population tested) the detective control should be.

The nature of fraud risks is such that there should be a systematic identification of the types of fraud schemes that can be perpetrated against or within the organization to identify the process controls needed to reduce and control the risks. Each industry is susceptible to different types of fraud schemes. The assessment becomes more cumbersome in organizations that span different industries. Organizations with multiple divisions/business units will need to first perform a broad organizationwide assessment and then perform more detailed and focused assessments of individual business units to identify the necessary process controls to detect fraud.

Proactive Fraud Detection Procedures

In addition to detective process controls, organizations may be able to use data analysis, continuous auditing techniques, and other technology tools effectively to detect fraudulent activity. Data analysis uses technology to identify anomalies, trends, and risk indicators within large populations of transactions. Users of this technology may be able to drill down into journal entries looking for suspicious transactions occurring at the end of a period or those that were made in one period and later reversed in the next period. These tools may also allow users to look for journal entries posted to revenue or expense accounts that improve net income to meet analysts' expectations or incentive compensation targets. Moreover, data analysis allows users to identify relationships among people, organizations, and events.

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 effective data analysis. Data analytics can also be used to cost-effectively ensure the effectiveness of other fraud preventive and detective controls.

Continuous auditing is the use of data analytics on a continuous or real-time basis, thereby allowing management or auditing to identify and report fraudulent activity more rapidly. For example, a Benford's Law analysis[39] 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" may promote quicker investigation of higher-risk transactions.

Technology tools enhance the ability of management at all levels to detect fraud. Data analysis, data mining, and digital analysis tools can:

- Identify hidden relationships among people, organizations, and events.
- Identify suspicious transactions.
- Assess the effectiveness of internal controls.

[39] Benford's Law analysis is a process of comparing actual results vs. expected results by looking for unusual transactions that do not fit an expected pattern.

- Monitor fraud threats and vulnerabilities.
- Consider and analyze thousands or millions of transactions.

Some auditors and consulting firms have developed tools, as part of their fraud detection efforts, that analyze journal entries to mitigate management override of the internal control system. These tools identify transactions subject to certain attributes that could indicate risk of management override, such as user identification, date of entry, and unusual account pairings.

Evidence of fraud can sometimes be found in e-mail as well. The ability of an organization to capture, maintain, and review the communications of any of its employees has led to the detection of numerous frauds in the past decade. This is accomplished through the use of strict and regular backup programs that capture data, not with the intent of uncovering fraud, but merely as a safeguard in the event that a retrospective search for evidence may be necessary. Recent amendments to the U.S. Federal Rules of Civil Procedure could affect future policy decisions about the retention of backup materials. The benefit of backup for business purposes, compared to a possible obligation to provide evidence in discovery, will need to be balanced in an organization's risk analysis.

As organizations grow and technology needs change, so do the opportunities for fraud. Because all fraud and misconduct schemes cannot be fought with the same tools and techniques, the organization periodically will need to assess the effectiveness of process controls, anonymous reporting, and internal auditing.

DOCUMENTATION OF FRAUD DETECTION TECHNIQUES

An organization should document the techniques developed and implemented to detect fraud. This includes documenting processes used to monitor the performance of fraud detective controls or to indicate when such controls are ineffective. Testing procedures conducted to ensure adequate operation of fraud detective controls and the test results should also be documented thoroughly.

Paramount to this documentation is a detailed description of the elements of the organization's fraud detection techniques, with emphasis placed on the roles and responsibilities of all parties involved. Organizations should designate and document the individuals and departments responsible for:

- Designing and planning the overall fraud detection process.
- Designing specific fraud detection controls.
- Implementing specific fraud detection controls.
- Monitoring specific fraud detection controls and the overall system of these controls for realization of the process objectives.
- Receiving and responding to complaints related to possible fraudulent activity.
- Investigating reports of fraudulent activity.
- Communicating information about suspected and confirmed fraud to appropriate parties.
- Periodically assessing and updating the plan for changes in technology, processes, and organization.

Although the organization may want to describe and explain some aspects of its fraud detection techniques to its employees, vendors, and stakeholders to promote deterrence, there will be aspects of the plan that the organization will want to remain confidential. During the fraud detection development phase, participants should be warned to

keep such information confidential. The board should approve a specific list of individuals who are permitted access to the information and define its own level of information access related to fraud detection controls.

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

ASSESSING THE ORGANIZATION'S FRAUD DETECTION

Organizations just beginning to assess their fraud risk management program, as well as those striving to improve their fraud risk management program, should conduct overall assessments of their fraud detection techniques. The Fraud Detection Scorecard in Appendix G can be used to assess how comprehensive the organization's detective controls are and how well they are working. Organizations periodically should reassess their fraud detection techniques to ensure that progress is being made to get to an "all-green" fraud detection status and that no elements of fraud detection are deteriorating. Organizations with strong commitments to fraud detection may also wish to engage independent outside experts to assess their fraud detection techniques.

CONTINUOUS MONITORING OF FRAUD DETECTION

The organization should develop ongoing monitoring and measurements to evaluate, remedy, and continuously improve the organization's fraud detection techniques. If deficiencies are found, management should ensure that improvements and corrections are made as soon as possible. Management should institute a follow-up plan to verify that corrective or remedial actions have been taken.

The organization should establish measurement criteria to monitor and improve fraud detection. These measures should be provided to the board on an ongoing basis.

Measurable criteria include the:

- Number of known fraud schemes committed against the organization.
- Number and status of fraud allegations received by the organization that required investigation.
- Number of fraud investigations resolved.
- Number of employees who have/have not signed the corporate ethics statement.
- Number of employees who have/have not completed ethics training sponsored by the organization.
- Number of whistleblower allegations received via the organization's hotline.
- Number of allegations that have been raised by other means.
- Number of messages supporting ethical behavior delivered to employees by executives.
- Number of vendors who have/have not signed the organization's ethical behavior requirements.
- Benchmarks with global fraud surveys, including the type of fraud experienced and average losses.
- Number of customers who have signed the organization's ethical behavior requirements.
- Number of fraud audits performed by internal auditors.

- Results of employee or other stakeholder surveys concerning the integrity or culture of the organization.
- Resources used by the organization.

Appropriate measurement techniques will vary by organization based on factors, such as controls in place, fraud risks identified, and resources available. Examples of specific measurement techniques are:

- The recurrence of frauds uncovered.
- The timeliness of implementation of remediation plans.
- Timeliness in implementing additional controls to prevent new frauds.
- Assessment of the likelihood that frauds perpetrated against other organizations in the same industry will occur in the organization.
- Comparison of fraud versus complaints, grievances, etc., via hotline calls.
- Comparison of the number of frauds discovered versus the number of fraud audits performed.
- Ratios of problems revealed in background checks versus the number of checks performed.

A senior member of management should be assigned as the process owner for each technique implemented. Each process owner should:

- Evaluate the effectiveness of the technique regularly.
- Adjust the technique as required.
- Document any adjustments.
- Report immediately through the appropriate channels details of any modification necessary or any technique that becomes less effective.

SECTION 5: FRAUD INVESTIGATION AND CORRECTIVE ACTION

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.

It is essential that any violations, deviations, or other breaches of the code of conduct or controls, regardless of where in the organization, or by whom, they are committed, be reported and dealt with in a timely manner. Appropriate punishment must be imposed, and suitable remediation completed. The board should ensure that the same rules are applied at all levels of the organization, including senior management.

FRAUD INVESTIGATION AND RESPONSE PROTOCOLS

Receiving the Allegation

Potential fraud may come to the organization's attention in many ways, including tips from employees, customers, or vendors; internal audits; process control identification; external audits; or by accident. The board should ensure that the organization develops a system for prompt, competent, and confidential review, investigation, and resolution of allegations involving potential fraud or misconduct. Protocols for the board's involvement in such cases — which

will vary depending on the nature, potential impact, and seniority of persons involved — should be defined clearly and communicated to management by the board.

The investigation and response system should include a process for:

- Categorizing issues.
- Confirming the validity of the allegation.
- Defining the severity of the allegation.
- Escalating the issue or investigation when appropriate.
- Referring issues outside the scope of the program.
- Conducting the investigation and fact-finding.
- Resolving or closing the investigation.
- Listing types of information that should be kept confidential.
- Defining how the investigation will be documented.
- Managing and retaining documents and information.

The process approved by the board should include a tracking or case management system in which all allegations of fraud are logged. Designated senior management approved by the board and the board itself may be given access to this system if necessary to ensure that appropriate action is being taken.

Evaluating the Allegation

Once an allegation is received, the organization should follow the process approved by the board to evaluate the allegation. The process should include designating an individual or individuals with the necessary authority and skills to conduct an initial evaluation of the allegation and 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 advisers to assist in this evaluation.

The allegation should be examined to determine whether it involves a potential violation of law, rules, or company policy. Depending on the nature and severity of the allegation, other departments may need to be consulted, such as HR, legal counsel, senior management, IT, internal auditing, security, or loss prevention. The organization's external auditor must also be advised of any fraud that could affect the organization's financial statements.

If an allegation involves senior management, or if the allegation affects the financial statements, there may be standards, regulations, or laws that require that others (e.g., audit committee, board, external auditors, counsel) be notified of the allegation. For example, if the allegation relates to misconduct involving the CEO, the board should be notified of the allegation and should ensure that the CEO is not overseeing the investigation.

Investigation Protocols

Investigations should be performed in accordance with protocols approved by the board. A consistent process for conducting investigations can help the organization mitigate losses and manage risks associated with the investigation.

Factors to consider in developing the investigation plan include:

- *Time-sensitivity* — Investigations may need to be conducted timely due to legal requirements, to mitigate losses or potential harm, or to institute an insurance claim.
- *Notification* — Certain allegations may require notification to regulators, law enforcement, insurers, or external auditors.
- *Confidentiality* — Information gathered needs to be kept confidential and distribution limited to those with an established need.
- *Legal privileges* — Involving legal counsel early in the process or, in some cases, in leading the investigation, will help safeguard work product and attorney-client communications.
- *Compliance* — Investigations should comply with applicable laws and rules regarding gathering information and interviewing witnesses.
- *Securing evidence* — Evidence should be protected so that it is not destroyed and so that it is admissible in legal proceedings.
- *Objectivity* — The investigation team should be removed sufficiently from the issues and individuals under investigation to conduct an objective assessment.
- *Goals* — Specific issues or concerns should appropriately influence the focus, scope, and timing of the investigation.

Responsibility for overseeing an investigation should be given to an individual with a level of authority at least one level higher than anyone potentially involved in the matter. Investigations of allegations involving senior management should be overseen by the board or a committee of the board designated for that purpose. Legal counsel may be appointed to supervise the investigation.

Depending on the specifics of the allegation, the investigation team may need to include members of different departments or disciplines to provide the knowledge and skill sets required. The following resources should be considered to determine whether their participation or assistance is necessary:

- Legal counsel.
- Fraud investigators.
- Internal auditors.
- External auditors.
- Accountants or forensic accountants.
- HR personnel.
- Security or loss prevention personnel.
- IT personnel.
- Computer forensics specialists.
- Management representative.

The investigation team leader should coordinate the investigation and interface with management as necessary. The roles and responsibilities of each team member should be communicated clearly. All team members should consider whether there is an actual or potential conflict of interest with any of the issues or parties that could be involved. Should the organization not have adequate internal resources and/or if it is determined that internal resources are not sufficiently objective, consideration should be given to retaining outside expertise.

CONDUCTING THE INVESTIGATION

Planning is essential to a thorough and competent investigation. The investigation team should establish the investigation tasks and assign each task to the appropriate team members. The plan should prioritize the performance of tasks to provide an interim report of findings, if necessary, and to revise or plan next steps. It is at this stage that appropriate consideration be given to legal issues and constraints in dealing with employees and third parties, obtaining relevant information, and documentation, including seeking assistance from the courts and monitoring the integrity of the results of the investigation, thereby maximizing the prospects of success.

Investigations generally include many of the following tasks:

1) Interviewing, including:
    a) Neutral third-party witnesses.
    b) Corroborative witnesses.
    c) Possible co-conspirators.
    d) The accused.

2) Evidence collection, including:
    a) Internal documents, such as
        i) Personnel files.
        ii) Internal phone records.
        iii) Computer files and other electronic devices.
        iv) E-mail.
        v) Financial records.
        vi) Security camera videos.
        vii) Physical and IT system access records.
    b) External records, such as
        i) Public records.
        ii) Customer/vendor information.
        iii) Media reports.
        iv) Information held by third parties.
        v) Private detective reports.

3) Computer forensic examinations.

4) Evidence analysis, including:
    a) Review and categorization of information collected.
    b) Computer-assisted data analysis.
    c) Development and testing of hypotheses.

The investigation team should document and track the steps of the investigation, including:

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

REPORTING THE RESULTS

The investigation team should report its findings to the party overseeing the investigation, such as senior management, directors, or legal counsel. Where legal counsel is supervising the investigation, counsel will determine the appropriate form of the report. The nature and distribution of the report may be affected by the goals of protecting legal privileges and avoiding defamatory statements. For similar reasons, advice of counsel should be sought before the party overseeing the investigation makes public statements or other communications regarding the investigation.

CORRECTIVE ACTION

After the investigation has been completed, the organization will need to determine what action to take in response to the findings. Any findings of actual or potential material impact may need to be reported to the board, the audit committee, and the external auditor if they are not receiving investigation reports directly. Notification may also be required to legal and regulatory agencies and the organization's insurers.

In some cases it may be necessary to take certain actions before the investigation is complete (e.g., to preserve evidence, maintain confidence, or mitigate losses). This could require suspension or reassignment of individuals or legal actions to restrain assets. Those responsible for such decisions should ensure there is a sufficient basis for those actions.

Any action taken should be appropriate under the circumstances, applied consistently to all levels of employees, including senior management, and should be taken only after consultation with individuals responsible for such decisions. Management consultation with legal counsel is strongly recommended before taking disciplinary, civil, or criminal action.

Possible actions include one or more of the following:

- Criminal referral — The organization may refer the case to law enforcement voluntarily, and, in some cases, it 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. An appropriate member of senior management, such as the chief legal counsel, should be authorized to make the decision as to whether pursuing criminal prosecution is appropriate.
- Civil action — The organization may wish to pursue its own civil action against the perpetrators to recover funds.
- Disciplinary action — Internal disciplinary action may include termination, suspension (with or without pay), demotion, or warnings.
- Insurance claim — The organization may be able to pursue an insurance claim for some or all of its losses.

- Extended investigation — Conducting a root cause analysis and performing an extended investigation may identify similar misconduct elsewhere in the organization.
- 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 in the future.
- Internal control remediation — The organization may wish to enhance certain internal controls to reduce the risk of similar frauds going undetected in the future.

The organization should consider the potential impact of its response and the message that it may send to the public, stakeholders, and others.

MEASUREMENT

The scale and complexity of fraud investigations often varies considerably, requiring some flexibility or customization for the measurements adopted. Although a variety of measures can be applied, the following may be relatively simple and powerful measurements to track:

- Issue resolution time (average number of days to resolve an issue) — This can be measured separately for different categories of incident to avoid creating pressure to resolve complex cases in an unrealistically short time.
- 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.
- Value of losses recovered and future losses prevented — Fraud investigations are important for their deterrent effect, so their cost-effectiveness should not be judged merely by the assets they help to recover. However, pursuing asset recoveries vigorously and estimating future losses prevented can help to demonstrate the value of fraud risk management actions.

CONCLUDING COMMENTS

A proactive approach to managing fraud risk is one of the best steps organizations can take to mitigate exposure to fraudulent activities. Although complete elimination of all fraud risk is most likely unachievable or uneconomical, organizations can take positive and constructive steps to reduce their exposure. The combination of effective fraud risk governance, a thorough fraud risk assessment, strong fraud prevention and detection (including specific anti-fraud control processes), as well as coordinated and timely investigations and corrective actions, can significantly mitigate fraud risks.

Although fraud is not a subject that any organization wants to deal with, the reality is most organizations experience fraud to some degree. The important thing to note is that dealing with fraud can be constructive, and forward-thinking, and can position an organization in a leadership role within its industry or business segment. Strong, effective, and well-run organizations exist because management takes proactive steps to anticipate issues before they occur and to take action to prevent undesired results. Implementation of this guide should help establish a climate where positive and constructive steps are taken to protect employees and ensure a positive culture. It should be recognized that the dynamics of any organization require an ongoing reassessment of fraud exposures and responses in light of the changing environment the organization encounters.

APPENDIX A: REFERENCE MATERIAL

FOR EXECUTIVES

American Institute of Certified Public Accountants (AICPA), *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention*, 2005, www.aicpa.org.

Association of Certified Fraud Examiners (ACFE)/AICPA, *Fraud Tools*, www.acfe.com.

Canadian Institute of Chartered Accountants (CICA), *20 Questions Directors Should Ask About Codes of Conduct*, www.cica.ca.

Corporate Executive Board, *A Constant Vigilance, Safeguarding the Corporation from Fraud and Abuse*, Audit Directors Roundtable Research Findings, 2005.

I.J. Alexander Dyck, Adair Morse, and Luigi Zingales, "Who Blows the Whistle on Corporate Fraud?", CRSP Working Paper No. 618, January 2007, www.ssrn.com/abstract=959410.

Robert Tillman and Michael Inderguard, *Control Overrides in Financial Statement Fraud, A Report to the Institute for Fraud Prevention*, 2007, St. John's University, www.theifp.org.

U.S. Securities and Exchange Commission, *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* (Release Nos. 33-8810, 34-55929, FR-77; File No. S7-24-06; June 27, 2007), www.sec.gov.

FRAUD RISKS

ACFE, *2006 ACFE Report to the Nation on Occupational Fraud & Abuse*, 2006, www.acfe.com.

Ernst & Young LLP, "9th Global Fraud Survey, Fraud Risk in Emerging Markets," 2006, www.ey.com.

Transparency International, "TI Corruption Perceptions Index," 2007, www.transparency.org.

U.S. Department of Justice, "Principles of Federal Prosecution of Business Organizations," 2006, www.usdoj.gov.

FRAUD CONTROLS

Deloitte Forensic Center, *Ten Things About Fraud Control: How Executives View the "Fraud Control Gap,"* 2007, www.deloitte.com.

Ethisphere Council, *43 Considerations for Writing, Reviewing or Revising a Code of Conduct*, www.ethisphere.com.

KPMG LLP, *Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response*, 2006, www.us.kpmg.com.

Open Compliance and Ethics Group (OCEG), *Foundation Guidelines Red Book*, 2007, www.oceg.org.

OCEG, *Hotline/Helpline Guide: Designing, Managing, and Measuring Hotlines/Helplines*, 2006, www.oceg.org.

OCEG, *Internal Audit Guide: Evaluating a Compliance and Ethics Program*, 2006, www.oceg.org.

OCEG, *Measurement & Metrics Guide: Performance Measurement Approach and Metrics for a Compliance and Ethics Program*, 2006, www.oceg.org.

PricewaterhouseCoopers LLP, *Key Elements of Antifraud Programs & Controls*, 2003, www.pwc.com.

Security Executive Council, *2007 Corporate Governance and Compliance Hotline Benchmarking Report*, 2007, www.securityexecutivecouncil.com.

The Network, *Best Practices in Ethics Hotlines*, 2006, www.tnwinc.com.

U.S. Sentencing Commission, *2005 Federal Sentencing Guidelines Manual*, Chapter Eight: Sentencing of Organizations, 2005, www.ussc.gov.

INTERNAL AUDITING

The Institute of Internal Auditors (IIA), *Definition of Internal Auditing*, www.theiia.org.

The IIA, *Practice Advisory 1210.A2-1: Auditor's Responsibilities Relating to Fraud Risk Assessment, Prevention, and Detection,* www.theiia.org.

The IIA, *Practice Advisory 1210.A2-2: Auditor's Responsibilities Relating to Fraud Investigation, Reporting, Resolution, and Communication,* www.theiia.org.

The IIA–UK and Ireland, *Fraud Position Statement,* www.iia.org.uk.

GENERAL

ACFE, *2007 Fraud Examiners Manual*, 2007.

ALARM (The National Forum for Risk Management in the Public Sector (UK)), *Managing the Risk of Fraud*.

Ted Avey, Ted Baskerville, and Alan Brill, *The CPA's Handbook of Fraud and Commercial Crime Prevention*, AICPA, 2000.

CICA, *The Accountant's Handbook of Fraud and Commercial Crime*, www.cica.ca.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Report of the National Commission on Fraudulent Financial Reporting (Treadway Report)*, 1987, www.coso.org.

HM Treasury, Assurance, Control, and Risk, *Managing the Risk of Fraud: A Guide for Managers*, 2003, www.hm-treasury.gov.uk.

International Federation of Accountants, *Defining and Developing an Effective Code of Conduct for Organizations*, June 2007, www.ifac.org.

IT Policy Compliance Group, *Why Compliance Pays: Reputations and Revenues at Risk, Benchmark Research Report*, 2007, www.itpolicycompliance.com.

Sarbanes-Oxley Act of 2002, 107th U.S. Cong., 2nd session (January 2002), H.R. 3763, www.sarbanes-oxley.com.

The Chartered Institute of Management Accountants, *Fraud Risk Management–A Guide to Good Practice*, 2001, www.cimaglobal.com.

The Chartered Institute of Public Finance and Accountancy (UK), *Managing the Risk of Fraud – Actions to Counter Fraud and Corruption (updated 2008)*.

UK Financial Services Authority, *Firms' High-Level Management of Fraud Risk*, 2006, www.fsa.gov.uk.

Joseph T. Wells, *Corporate Fraud Handbook*, 2nd edition, Wiley, 2007.

APPENDIX B: SAMPLE FRAMEWORK FOR A FRAUD CONTROL POLICY (OR PLAN)[40]

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

1. EXECUTIVE SUMMARY

Definition of *fraud*
Statement of attitude to fraud
Code of conduct (relationship to)
Relationship with entity's other plans
Roles and accountabilities

2. SUMMARY OF FRAUD CONTROL STRATEGIES

Appointment of fraud control officer
External assistance to the fraud control officer
Fraud control responsibilities
Fraud risk management (including fraud risk assessment)
Fraud awareness
Fraud detection
Fraud reporting
Investigation of fraud and other improper conduct
Internal control review following discovery of fraud
Fidelity guarantee and criminal conduct insurance
Internal audit program

3. FRAUD RISK MANAGEMENT

Regular program for fraud risk assessment
Ongoing review of fraud control strategies
Fraud risk assessment
Implementation of proposed actions

4. PROCEDURES FOR REPORTING FRAUD

Internal reporting
Reports by members of staff
Protection of employees reporting suspected fraud
External anonymous reporting

[40] This sample is provided by The Australian Standard on Fraud and Corruption Control, AS 8001-2003. Please note that other definitions of *fraud* exist, and thus it is important for the organization to explain clearly what types of transactions or activities are covered by the policy.

Reports to the police
Reports to external parties
Administrative remedies
Recovery of the proceeds of fraudulent conduct
Reporting requirements

5. EMPLOYMENT CONDITIONS

Pre-employment screening
Annual leave

6. CONFLICT OF INTEREST

The impact of conflicts of interest
Register of interests
Conflict of interest policy

7. PROCEDURES FOR FRAUD INVESTIGATION

Internal investigations
External investigative resources
Documentation of the results of the investigation

8. INTERNAL AUDIT STRATEGY

Internal audit capability
Internal audit fraud control function

9. REVIEW OF FRAUD CONTROL ARRANGEMENTS

APPENDIX C: SAMPLE FRAUD POLICY[41]

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

BACKGROUND	The corporate fraud policy is established to facilitate the development of controls that will aid in the detection and prevention of fraud against ABC Corporation. It is the intent of ABC Corporation to promote consistent organizational behavior by providing guidelines and assigning responsibility for the development of controls and conduct of investigations.
SCOPE OF POLICY	This policy applies to any irregularity, or suspected irregularity, involving employees as well as shareholders, consultants, vendors, contractors, outside agencies doing business with employees of such agencies, and/or any other parties with a business relationship with ABC Corporation (also called the Company). Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.
POLICY	Management is responsible for the detection and prevention of fraud, misappropriations, and other irregularities. *Fraud* is defined as the intentional, false representation or concealment of a material fact for the purpose of inducing another to act upon it to his or her injury. Each member of the management team will be familiar with the types of improprieties that might occur within his or her area of responsibility and be alert for any indication of irregularity. Any irregularity that is detected or suspected must be reported immediately to the Director of _____, who coordinates all investigations with the Legal Department and other affected areas, both internal and external.

[41] This sample is provided by the Association of Certified Fraud Examiners' Sample Fraud Policy. Please note that other definitions of fraud exist, and thus it is important for the organization to explain clearly what types of transactions or activities are covered by the policy.

ACTIONS CONSTITUTING FRAUD

The terms *defalcation, misappropriation,* and *other fiscal irregularities* refer to, but are not limited to:

- Any dishonest or fraudulent act.
- Misappropriation of funds, securities, supplies, or other assets.
- Impropriety in the handling or reporting of money or financial transactions.
- Profiteering as a result of insider knowledge of company activities.
- Disclosing confidential and proprietary information to outside parties.
- Disclosing to other persons securities activities engaged in or contemplated by the company.
- Accepting or seeking anything of material value from contractors, vendors, or persons providing services/materials to the Company. Exception: Gifts less than US $50 in value.
- Destruction, removal, or inappropriate use of records, furniture, fixtures, and equipment.
- Any similar or related irregularity.

OTHER IRREGULARITIES

Irregularities concerning an employee's moral, ethical, or behavioral conduct should by resolved by departmental management and the Employee Relations Unit of Human Resources rather than the _____ Unit.

If there is any question as to whether an action constitutes fraud, contact the Director of _____ for guidance.

INVESTIGATION RESPONSIBILITIES

The _____ Unit has the primary responsibility for the investigation of all suspected fraudulent acts as defined in the policy. If the investigation substantiates that fraudulent activities have occurred, the _____ Unit will issue reports to appropriate designated personnel and, if appropriate, to the Board of Directors through the Audit Committee.

Decisions to prosecute or refer the examination results to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with legal counsel and senior management, as will final decisions on disposition of the case.

CONFIDENTIALITY

The _____ Unit treats all information received confidentially. Any employee who suspects dishonest or fraudulent activity will notify the _____ Unit immediately, and should not attempt to personally conduct investigations or interviews/interrogations related to any suspected fraudulent act (see Reporting Procedures section below).

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the Company from potential civil liability.

AUTHORIZATION FOR INVESTIGATING SUSPECTED FRAUD

Members of the Investigation Unit will have:

- Free and unrestricted access to all Company records and premises, whether owned or rented.
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

REPORTING PROCEDURES

Great care must be taken in the investigation of suspected improprieties or irregularities so as to avoid mistaken accusations or alerting suspected individuals that an investigation is under way.

An employee who discovers or suspects fraudulent activity will contact the _____ Unit immediately. The employee or other complainant may remain anonymous. All inquiries concerning the activity under investigation from the suspected individual, his or her attorney or representative, or any other inquirer should be directed to the Investigations Unit or the Legal Department. No information concerning the status of an investigation will be given out. The proper response to any inquiries is: "I am not at liberty to discuss this matter." Under no circumstances should any reference be made to "the allegation," "the crime," "the fraud," "the forgery," "the misappropriation," or any other specific reference.

The reporting individual should be informed of the following:

- Do not contact the suspected individual in an effort to determine facts or demand restitution.
- Do not discuss the case, facts, suspicions, or allegations with anyone unless specifically asked to do so by the Legal Department or _____ Unit.

TERMINATION	If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed for approval by the designated representatives from Human Resources and the Legal Department and, if necessary, by outside counsel, before any such action is taken. The _____ Unit does not have the authority to terminate an employee. The decision to terminate an employee is made by the employee's management. Should the _____ Unit believe the management decision inappropriate for the facts presented, the facts will be presented to executive-level management for a decision.
ADMINISTRATION	The Director of _____ is responsible for the administration, revision, interpretation, and application of this policy. The policy will be reviewed annually and revised as needed.
APPROVAL	_____ (CEO/Senior Vice President/Executive) _____ Date

SAMPLE FRAUD POLICY DECISION MATRIX

NOTE: This matrix can be used as a tool to summarize and visualize the responsibilities that have been defined for the organization. This is not a standard for "who" should have "what" responsibilities.

Action Required	Investigation Unit	Internal Auditing	Finance Acctg.	Exec Mgmt.	Line Mgmt.	Risk Mgmt.	PR	Employee Relations	Legal
1. Controls to Prevent Fraud	S	S	S	P	SR	S	S	S	S
2. Incident Reporting	P	S	S	S	S	S	S	S	S
3. Investigation of Fraud	P	S						S	S
4. Referrals to Law Enforcement	P								S
5. Recovery of Monies Due to Fraud	P								
6. Recommendations to Prevent Fraud	SR	SR	S	S	S	S	S	S	S
7. Internal Control Reviews		P							
8. Handle Cases of a Sensitive Nature	P	S		S		S		S	S
9. Publicity/Press Releases	S	S					P		
10. Civil Litigation	S	S							P
11. Corrective Action/ Recommendations to Prevent Recurrences	SR	SR		S	SR	S			S
12. Monitor Recoveries	S		P						
13. Proactive Fraud Auditing	S	P							
14. Fraud Education/ Training	P	S			S		S		
15. Risk Analysis of Areas of Vulnerability	S	S				P			
16. Case Analysis	P	S							
17. Hotline	P	S							
18. Ethics Line	S	S							P

P (Primary Responsibility) **S (Secondary Responsibility)** **SR (Shared Responsibility)**

APPENDIX D: FRAUD RISK ASSESSMENT FRAMEWORK EXAMPLE

NOTE: This example is for illustrative purposes and focuses solely on potential revenue recognition risks within financial reporting. A full fraud risk assessment would consider fraudulent financial reporting in other areas relevant to the organization, such as accounts subject to estimation, related-party transactions, and inventory accounting. In addition, the risk of misappropriation of assets, corruption, and other misconduct would be assessed in the same manner.

Identified Fraud Risks and Schemes (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Existing Anti-fraud Controls (5)	Controls Effectiveness Assessment (6)	Residual Risks (7)	Fraud Risk Response (8)
Financial Reporting Revenue recognition • Backdating agreements	Reasonably possible	Material	Sales personnel	Controlled contract administration system	Tested by IA	N/A	Periodic testing by IA
• Channel stuffing	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Holding books open	Reasonably possible	Material	Accounting	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 Tested by management Tested by IA Tested by IA	Risk of management override	Testing of late journal entries Cut off testing by IA
• Late shipments	Reasonably possible	Significant	Shipping dept.	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 Tested by management Tested by IA	Risk of management override	Cut off testing by IA
• Side letters/ agreements	Probable	Material	Sales personnel	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	Tested by management Tested by management	Risk of override	Disaggregated analysis of sales, sales returns, and adjustments by salesperson
• Inappropriate journal entries	Reasonably possible	Material	Accounting & Finance	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 nonstandard entries subject to two levels of review	Tested by IA Tested by IA Tested by management	Risk of override N/A N/A	Data mining of journal entry population by IA for: • Unusual Dr/CR combinations • Late entries to accounts subject to estimation

Identified Fraud Risks and Schemes (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Existing Anti-fraud Controls (5)	Controls Effectiveness Assessment (6)	Residual Risks (7)	Fraud Risk Response (8)
• Roundtrip transactions	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Manipulation of bill and hold arrangements	Remote	Insignificant	N/A	N/A	N/A	N/A	N/A
• Early delivery of product	Reasonably possible	Significant	Sales and shipping	Systematic matching of sales order to shipping documentation; exception reports generated.	Tested by management	Adequately mitigated by controls	N/A
• Partial shipments	Reasonably possible	Significant	Sales and shipping	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	Adequately mitigated by controls	N/A
• Additional revenue risks				Systematic shipping documents manually checked against every shipment.			

1. Identified Fraud Risks and Schemes: This column should include a full list of the potential fraud risks and schemes that may face the organization. This list will be different for different organizations and should be informed by (a) industry research, (b) interviews of employees and other stakeholders, (c) brainstorming sessions, and (d) activity on the whistleblower hotline.
2. Likelihood of Occurrence: To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the organization establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of the assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.
3. Significance to the Organization: Quantitative and qualitative factors should be considered when assessing the 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 assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.
4. People and/or Department Subject to the Risk: As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the organization are subject to the risk. This knowledge will assist the organization in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of authority, and proactive fraud auditing procedures.
5. Existing Anti-fraud Internal Controls: Map pre-existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for 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. Assessment of Internal Controls Effectiveness: The organization should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks as intended. Companies subject to the provisions of The U.S. Sarbanes-Oxley Act of 2002 Section 404 will have a process such as this in place. Organizations not subject to Sarbanes-Oxley should consider what review and monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.
7. Residual Risks: After consideration of the internal control structure, it may be determined that certain 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. These residual risks should be evaluated by the organization in the development of the fraud risk response.
8. Fraud Risk Response: Residual risks should be evaluated by the organization and fraud risk responses should be designed to address such remaining risk. The fraud risk response could be one or a combination of the following: (a) implementing additional controls, (b) designing proactive fraud auditing techniques, and/or (c) reducing the risk by exiting the activity.

APPENDIX E: FRAUD RISK EXPOSURES[42]

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

The following illustrates the types of frauds an organization might encounter. This listing is not meant to be all-inclusive but to provide a starting point for an organization to identify which areas are vulnerable to fraud. More attention will be needed to identify specific industry, location, and cultural factors that can influence fraudulent behavior. Once identified, the fraud risk assessment framework shown in Appendix D could be used[43].

1) Intentional manipulation of financial statements can lead to:
    a) Inappropriately reported revenues
        (1) Fictitious revenues
        (2) Premature revenue recognition
        (3) Contract revenue and expense recognition
    b) Inappropriately reported expenses
        (1) Period recognition of expenses
    c) Inappropriately reflected balance sheet amounts, including reserves
        (1) Improper asset valuation
            (a) Inventory
            (b) Accounts receivable
            (c) Mergers and acquisitions
            (d) Capitalization of intangible items
        (2) Misclassification of assets
        (3) Inappropriate depreciation methods
        (4) Concealed liabilities and expenses
            (a) Omission
            (b) Sales returns and allowances and warranties
            (c) Capitalization of expenses
            (d) Tax liability
    d) Inappropriately improved and/or masked disclosures
        (1) Liabilities omissions
        (2) Subsequent events
        (3) Related-party transactions
        (4) Accounting changes
        (5) Management frauds uncovered
        (6) Backdating transactions
    e) Concealing misappropriation of assets
    f) Concealing unauthorized receipts and expenditures
    g) Concealing unauthorized acquisition, disposition, and use of assets

[42] The *Fraud Risk Manual* issued by the ACFE, 2007.

[43] For a sample list of fraud schemes and potential controls to be installed to combat the fraud, see Appendix 8 of *Managing the Risk of Fraud: A Guide for Managers* by HM Treasury, in Appendix A of this paper.

2) Misappropriation of:
    a) Tangible assets by
        (1) Cash theft
            (a) Sales register manipulation
            (b) Skimming
            (c) Collection procedures
            (d) Understated sales
            (e) Theft of checks received
            (f) Check for currency substitution
            (g) Lapping accounts
            (h) False entries to sales account
            (i) Inventory padding
            (j) Theft of cash from register
            (k) Deposit lapping
            (l) Deposits in transit
        (2) Fraudulent disbursements
            (a) False refunds
            (b) False voids
            (c) Small disbursements
            (d) Check tampering
            (e) Billing schemes
            (f) Personal purchases with company funds
            (g) Returning merchandise for cash
        (3) Payroll fraud
            (a) Ghost employees
            (b) Falsified hours and salary
            (c) Commission sales
        (4) Expense reimbursement
            (a) Mischaracterized expenses
            (b) Overstated expenses
            (c) Fictitious expenses
            (d) Multiple reimbursements
        (5) Loans
            (a) Loans to nonexistent borrowers
            (b) Double pledged collateral
            (c) False application information
            (d) Construction loans
        (6) Real estate
            (a) Appraisal value
            (b) Fraudulent appraisal
        (7) Wire transfer
            (a) System password compromise
            (b) Forged authorizations
            (c) Unauthorized transfer account
            (d) ATM

(8) Check and credit card fraud
    (a) Counterfeiting checks
    (b) Check theft
    (c) Stop payment orders
    (d) Unauthorized or lost credit cards
    (e) Counterfeit credit cards
    (f) Mail theft
(9) Insurance fraud
    (a) Dividend checks
    (b) Settlement checks
    (c) Premium
    (d) Fictitious payee
    (e) Fictitious death claim
    (f) Underwriting misrepresentation
    (g) Vehicle insurance — staged accidents
    (h) Inflated damages
    (i) Rental car fraud
(10) Inventory
    (a) Misuse of inventory
    (b) Theft of inventory
    (c) Purchasing and receiving falsification
    (d) False shipments
    (e) Concealing inventory shrinkage

b) Intangible assets
(1) Theft of intellectual property
    (a) Espionage
    (b) Loss of information
    (c) Spying
    (d) Infiltration
    (e) Informants
    (f) Trash and waste disposal
    (g) Surveillance
(2) Customers
(3) Vendors
    c) Proprietary business opportunities

3) Corruption including:
a) Bribery and gratuities to
(1) Companies
(2) Private individuals
(3) Public officials

b) Embezzlement
    (1) False accounting entries
    (2) Unauthorized withdrawals
    (3) Unauthorized disbursements
    (4) Paying personal expenses from bank funds
    (5) Unrecorded cash payments
    (6) Theft of physical property
    (7) Moving money from dormant accounts
c) Receipt of bribes, kickbacks, and gratuities
    (1) Bid rigging
    (2) Kickbacks
        (a) Diverted business to vendors
        (b) Over billing
    (3) Illegal payments
        (a) Gifts
        (b) Travel
        (c) Entertainment
        (d) Loans
        (e) Credit card payments for personal items
        (f) Transfers for other than fair value
        (g) Favorable treatment
    (4) Conflicts of interest
        (a) Purchases
        (b) Sales
        (c) Business diversion
        (d) Resourcing
        (e) Financial disclosure of interest in vendors
        (f) Ownership interest in suppliers
d) FCPA violations
    (1) Anti-bribery provisions
    (2) Books and records violations
    (3) Internal control weaknesses
e) Money laundering
f) Aiding and abetting fraud by other parties (customers, vendors)

APPENDIX F: FRAUD PREVENTION SCORECARD

To assess the strength of the organization's fraud prevention system, carefully assess each area below and score the area, factor, or consideration as:

- Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level.
- Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level.
- Green: indicating that the area, factor, or consideration is strong and fraud risk has been reduced — at least — to a minimally acceptable level.

Each area, factor, or consideration scored either red or yellow should have a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our organizational culture — tone at the top — is as strong as it can possibly be and establishes a zero-tolerance environment with respect to fraud.		
Our organization's top management consistently displays the appropriate attitude regarding fraud prevention and encourages free and open communication regarding ethical behavior.		
Our Code of Organizational Conduct has specific provisions that address and prohibit inappropriate relationships whereby members of our board or members of management could use their positions for personal gain or other inappropriate purposes.		
We have done a rigorous fraud risk assessment using the COSO *Enterprise Risk Management–Integrated Framework* and have taken specific actions to strengthen our prevention mechanisms as necessary.		
We have assessed fraud risk for our organization adequately based on evaluations of similar organizations in our industry, known frauds that have occurred in similar organizations, in-house fraud brainstorming, and periodic reassessments of risk.		
We have addressed the strengths and weaknesses of our internal control environment adequately and have taken specific steps to strengthen the internal control structure to help prevent the occurrences of fraud.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our organizational structure contains no unnecessary entities that might be used for inappropriate purposes or that might enable less-than-arms-length transactions or relationships.		
We have assessed all overseas and decentralized operations carefully and have taken proactive steps to ensure that they have fraud preventive controls in place to conform with the strictest legal standards and highest ethical principles.		
We have divested our organization of all unnecessary third-party and related-party relationships.		
For any remaining third-party and related-party relationships, we have taken positive measures to ensure that such relationships do not allow opportunities for frauds to occur without detection.		
We have assessed the alignment of authorities and responsibilities at all levels of organization management and are not aware of any misalignments that might represent vulnerabilities to fraud.		
Our audit committee has taken a very proactive posture with respect to fraud prevention.		
Our audit committee is composed only of independent directors and includes persons with financial accounting and reporting expertise.		
Our audit committee meets at least quarterly and devotes substantial time to assessing fraud risk and proactively implementing fraud preventive mechanisms.		
We have a strong internal audit department (if applicable) that functions independently of management. The charter of our internal audit department expressly states that the internal audit team will help prevent and detect fraud and misconduct.		
We have designated an individual with the authority and responsibility for overseeing and maintaining our fraud prevention programs, and have given this individual the resources needed to manage our fraud prevention programs effectively. This individual has direct access to the audit committee.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our human resources department conducts background investigations with the specific objective of assuring that persons with inappropriate records or characters inconsistent with our corporate culture and ethics are identified and eliminated from the hiring process.		
Our human resources department conducts background investigations with respect to promotions or transfers into positions of responsibility.		
Personnel involved in the financial reporting process have been assessed with regard to their competencies and integrity and have been found to be of the highest caliber.		
All of our employees, vendors, contractors, and business partners have been made aware of our zero-tolerance policies related to fraud and are aware of the appropriate steps to take in the event that any evidence of possible fraud comes to their attention.		
We have a rigorous program for communicating our fraud prevention policies and procedures to all employees, vendors, contractors, and business partners.		
We have policies and procedures in place for authorization and approvals of certain types of transactions and for certain values of transactions to help prevent and detect the occurrences of fraud.		
Our performance measurement and evaluation process includes an element specifically addressing ethics and integrity as well as adherence to the Code of Organizational Conduct.		
All new hires must undergo rigorous ethics and fraud awareness and fraud prevention training.		
All employees must attend periodic (at least annual) ethics and fraud awareness and fraud prevention training, and the effectiveness of this training is affirmed through testing.		
Terminated, resigning, or retiring employees participate in an exit interview process designed to identify potential fraud and vulnerabilities to fraud that may be taking place in our organization. A specific focus of these interviews is an assessment of management's integrity and adherence to the Code of Organizational Conduct. All concerns resulting from these interviews are communicated to our audit committee.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
We have an effective whistleblower protection program and fraud hotline in place, and its existence and procedures are known to all employees, vendors, contractors, and business partners.		
We review the above fraud preventive mechanisms on an ongoing basis and document these reviews as well as the communication with the audit committee regarding areas that need improvement.		
We have a fraud response plan in place and know how to respond if a fraud allegation is made. The fraud response plan considers: • Who should perform the investigation. • How the investigation should be performed. • When a voluntary disclosure to the government should be made. • How to determine the remedial action. • How to remedy control deficiencies identified. • How to administer disciplinary action.		

APPENDIX G: FRAUD DETECTION SCORECARD

To assess the strength of the organization's fraud detection system, carefully assess each area below and score the area, factor, or consideration as:

- Red: indicating that the area, factor, or consideration needs substantial strengthening and improvement to bring fraud risk down to an acceptable level.
- Yellow: indicating that the area, factor, or consideration needs some strengthening and improvement to bring fraud risk down to an acceptable level.
- Green: indicating that the area, factor, or consideration is strong and fraud risk has been reduced — at least — to a minimally acceptable level.

Each area, factor, or consideration that scores either red or yellow should have a note associated with it that describes the action plan for bringing it to green on the next scorecard.

Fraud Prevention Area, Factor, or Consideration	Score	Notes
We have integrated our fraud detection system with our fraud prevention system in a cost-effective manner.		
Our fraud detection processes and techniques pervade all levels of responsibility within our organization, from the board of directors and audit committee, to managers at all levels, to employees in all areas of operation.		
Our fraud detection policies include communicating to employees, vendors, and stakeholders that a strong fraud detection system is in place, but certain critical aspects of these systems are not disclosed to maintain the effectiveness of hidden controls.		
We use mandatory vacation periods or job rotation assignments for employees in key finance and accounting control positions.		
We periodically reassess our risk assessment criteria as our organization grows and changes to make sure we are aware of all possible types of fraud that may occur.		
Our fraud detection mechanisms place increased focus on areas in which we have concluded that preventive controls are weak or are not cost-effective.		
We focus our data analysis and continuous auditing efforts based on our assessment of the types of fraud schemes to which organizations like ours (in our industry, or with our lines of business) are susceptible.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
We take steps to ensure that our detection processes, procedures, and techniques remain confidential so that ordinary employees — and potential fraud perpetrators — do not become aware of their existence.		
We have comprehensive documentation of our fraud detection processes, procedures, and techniques so that we maintain our fraud detection vigilance over time and as our fraud detection team changes.		
Our detective controls include a well-publicized and well-managed fraud hotline.		
Our fraud hotline program provides anonymity to individuals who report suspected wrongdoing.		
Our fraud hotline program includes assurances that employees who report suspected wrongdoing will not face retaliation. We monitor for retaliation after an issue has been reported.		
Our fraud hotline has a multilingual capability and provides access to a trained interviewer 24 hours a day, 365 days a year.		
Our fraud hotline uses a case management system to log all calls and their follow-up to resolution, is tested periodically by our internal auditors, and is overseen by the audit committee.		
Our fraud hotline program analyzes data received and compares results to norms for similar organizations.		
Our fraud hotline program is independently evaluated periodically for effectiveness and compliance with established protocols.		
We use a rigorous system of data analysis and continuous auditing to detect fraudulent activity.		
Our information systems/IT process controls include controls specifically designed to detect fraudulent activity, as well as errors, and include reconciliations, independent reviews, physical inspections/counts, analyses, audits, and investigations.		
Our internal audit department's charter includes emphasis on conducting activities designed to detect fraud.		
Our internal auditors participate in the fraud risk assessment process and plan fraud detection activities based on the results of this risk assessment.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our internal auditors report to the audit committee and focus appropriate resources on assessing management's commitment to fraud detection.		
Our internal audit department is adequately funded, staffed, and trained to follow professional standards, and our internal audit personnel possess the appropriate competencies to support the group's objectives.		
Our internal audit department performs risk-based assessments to understand motivation and where potential manipulation may take place.		
Our internal audit personnel are aware of, and are trained in, the tools and techniques of fraud detection, response, and investigation as part of their continuing education program.		
Our data analysis programs focus on journal entries and unusual transactions, and transactions occurring at the end of a period or those that were made in one period and reversed in the next period.		
Our data analysis programs identify journal entries posted to revenue or expense accounts that improve net income or otherwise serve to meet analysts' expectations or incentive compensation targets.		
We have systems designed to monitor journal entries for evidence of possible management override efforts intended to misstate financial information.		
We use data analysis, data mining, and digital analysis tools to: (a) identify hidden relationships among people, organizations, and events; (b) identify suspicious transactions; (c) assess the effectiveness of internal controls; (d) monitor fraud threats and vulnerabilities; and (e) consider and analyze large volumes of transactions on a real-time basis.		
We use continuous auditing techniques to identify and report fraudulent activity more rapidly, including Benford's Law analysis to examine expense reports, general ledger accounts, and payroll accounts for unusual transactions, amounts, or patterns of activity that may require further analysis.		
We have systems in place to monitor employee e-mail for evidence of potential fraud.		

Fraud Prevention Area, Factor, or Consideration	Score	Notes
Our fraud detection documentation identifies the individuals and departments responsible for: • Designing and planning the overall fraud detection process. • Designing specific fraud detective controls. • Implementing specific fraud detective controls. • Monitoring specific fraud detective controls and the overall system of these controls for realization of the process objectives. • Receiving and responding to complaints related to possible fraudulent activity. • Investigating reports of fraudulent activity. • Communicating information about suspected and confirmed fraud to appropriate parties. • Periodically assessing and updating the plan for changes in technology, processes, and organization.		
We have established measurement criteria to monitor and improve compliance with fraud detective controls, including: • Number of, and loss amounts from, known fraud schemes committed against the organization. • Number and status of fraud allegations received by the organization that required investigation. • Number of fraud investigations resolved. • Number of employees who have signed the corporate ethics statement. • Number of employees who have completed ethics training sponsored by the organization. • Number of whistleblower allegations received via the organization's hotline. • Number of messages supporting ethical behavior delivered to employees by executives. • Number of vendors who have signed the organization's ethical behavior policy. • Number of customers who have signed the organization's ethical behavior policy. • Number of fraud audits performed by internal auditors.		
We periodically assess the effectiveness of our fraud detection processes, procedures, and techniques; document these assessments; and revise our processes, procedures, and techniques as appropriate.		

APPENDIX H: OCEG FOUNDATION PRINCIPLES THAT RELATE TO FRAUD

NOTE: This appendix is a sample from another entity. As such, no adjustment has been made to this material. The information may or may not agree with all the concepts noted within this paper. The material is being provided as an example that may be a used as a tool, reference, or starting point.

Below is a summary listing of the practices in the Open Compliance and Ethics Group (OCEG) Foundation[44] and how each practice serves the principles of establishing a strong fraud prevention program as advocated in this paper.

C-CULTURE

C1-Ethical Culture

C1.1 Define Principles & Values that reflect a desire for high ethical standards and a no tolerance position toward fraud and corruption.

C1.2 Enhance Ethical Climate & Mindsets as a deterrent to fraudulent and corrupt conduct.

C1.3 Foster Ethical Leadership through rewards and acknowledgment as a model of appropriate conduct in the face of stressors that would potentially lead to fraudulent or corrupt behaviors.

C2-Risk Culture

C2.1 Define Philosophy & Style that communicates and cascades through the organization a no tolerance position on fraud risk and the existence of strong anti-fraud policies and controls.

C2.2 Enhance Risk Management Climate & Mindsets so that the workforce in addition to the board and senior management are attune to the stressors and circumstances that create fraud risk so it can be deterred and detected promptly.

C3-Governance Culture

C3.1 Define Governance Style & Approach to specify the desired level of board oversight and involvement in the anti-fraud program, including the thresholds that escalate incidents of fraud to higher levels of visibility, up to and including board attention.

C3.2 Enhance Governance Climate & Mindsets to ensure that accountability for managing fraud risk ripples up to the responsible board member or committee, regularly placing a discussion of the status of the fraud risk management program on the agenda.

C4-Workforce Culture

C4.1 Understand Workforce Management Philosophy & Style to include the aspects of workforce management that either contribute to or deter the risk of fraudulent or corrupt behaviors.

C4.2 Enhance Commitment to the Workforce & Competency by structuring policies and practices in hiring, training, performance evaluation, promotion, compensation, rewards/discipline, career advancement and termination or retirement to deter fraudulent and corrupt behavior, including practices that deal swiftly and decisively with incidents and protect whistleblowers from retribution.

C4.3 Enhance Workforce Satisfaction & Commitment to eliminate or mitigate stressors that create fraud and corruption risk.

[44] © Open Compliance and Ethics Group (2003-2007). OCEG Foundation (Redbook), Phoenix, Ariz.: OCEG (available for free download at www.oceg.org/view/foundation).

O-ORGANIZATION / PERSONNEL

O1-Leadership & Champions

O1.1 Define Leadership & Champion Responsibilities to include communicating how fraud risk management program objectives facilitate organizational objectives, how individuals contribute to achieving program objectives and why the program is and should be supported enterprise wide.

O1.2 Screen & Select Program Leadership & Champions to assure that the leaders and champions are qualified to serve as advocates for anti-fraud messaging based upon prior upstanding conduct or remorseful transformation from prior fraudulent/corrupt or otherwise inappropriate conduct.

O1.3 Enhance Champion Skills & Competencies to include a thorough understanding of fraud, stressors that trigger fraudulent conduct, and the scope, parameters and activities of the fraud risk management program.

O2-Oversight Personnel

O2.1 Define Oversight Structure & Responsibilities to:

- include in the appropriate charter documents whether the entire board, a board member, or a board committee has been assigned oversight responsibilities for directing the activities of the fraud risk management program,
- evidence a commitment to a proactive approach to fraud risk management.
- play an active role in the risk assessment process, and using internal audit, and external auditors, as monitors of fraud risks.
- appoint one executive-level member of management to be responsible for fraud risk management.
- approve sufficient resources in the budget and long-range plans to enable the organization to achieve these objectives.
- ensure that management designs effective fraud risk management policies to encourage ethical behavior and to empower employees, customers, and vendors to insist those standards are met everyday.
- model good board governance practices (like board independence,) as a component of the fraud risk management program.
- require that the audit committee meet separately with the external audit firm and chief audit executive to discuss the results of the anti-fraud program on the entity's financial statements.
- ensure the board is receiving accurate and timely information from management, employees, internal and external auditors, and other stakeholders regarding potential fraud occurrences.
- assure protection of all requisite privileges and adherence to information management policy for communications related to fraud investigations and audit committee discussions.

O2.2 Screen & Select Oversight Personnel to identify the board member(s) best suited based upon skills, experience, knowledge, and character (based in part upon the results of background checks) to provide anti-fraud program oversight.

O2.3 Enhance Oversight Skills & Competencies so the board:

- has a thorough understanding of what constitutes fraud and corruption risk.
- sets the appropriate "tone at the top" in its own independent practices and through the CEO job description, evaluation, and succession-planning processes.
- maintains oversight of the fraud and corruption risk assessment.
- evaluates management's identification of fraud and corruption risks.

- leverages the experience of internal and external auditors regarding;
  - events or conditions that indicate incentives/pressures to perpetrate fraud, opportunities to carry out the fraud, or attitudes/rationalizations to justify a fraudulent action.
  - how and where they believe the entity's financial statements might be susceptible to material misstatement due to fraud.
  - inquires of management and others within the entity about the risks of fraud.
  - analytical procedures to identify unusual transactions or events, and amounts, ratios, and trends that might indicate matters that have financial statement implications.
- oversees the internal controls over financial reporting established by management.
- assesses the risk of financial fraud by management.
- ensures controls are in place to prevent, deter, and detect fraud by management.
- empowers the audit committee and external auditors to look for and report fraud of all sizes and types.

O2.4 Assess Oversight Personnel & Team Performance to include the effective exercise of oversight for the entity's fraud risk management program.

O3-Strategic Personnel

O3.1 Define Strategic Structure & Responsibilities using a job description that specifies the role with responsibility for, sufficient resources and authority to design and implement a fraud risk management program including the setting of policy, establishing of controls, training, implementing anti-fraud initiatives, processes for reporting and investigating alleged violations, and reporting to the board on the progress of program toward objectives, the status of investigations, activities in relation to detecting and mitigating incidents of fraudulent or corrupt behavior and any remedial steps for program improvement.

O3.2 Screen & Select Strategic Personnel to confirm that the individual vested with responsibility for the program is well-qualified and an appropriate model (as determined, in part, by a background check).

O3.3 Enhance Strategic Skills & Competencies in program management techniques like vision, mission and values development, risk assessment, program effectiveness and performance evaluations, control development, investigations management, as well as a thorough understanding of the organization's fraud risks and process level controls.

O3.4 Assess Strategic Personnel & Team Performance compared to fraud risk management program performance targets and individual performance targets.

O4-Operational Personnel

O4.1 Define Operational Structure & Responsibilities that address the fraud risk management responsibilities of all levels of operational personnel, including participate in the process of creating a strong control environment, designing and implementing control activities, and participate in monitoring activities, reporting incidences of fraud and corruption, paying particular attention to the unique roles of internal audit, compliance, ethics, and legal program implementation and investigation roles.

O4.2 Screen & Select Operational Personnel to confirm that the individuals vested with responsibility for various aspects of the fraud risk management program are not compromised in their effectiveness or unduly pose greater risk to the organization by virtue of past violations of ethical standards and/or unlawful behavior.

O4.3 Enhance Operational Skills & Competencies through training and understanding of:

- their role within the internal control framework and in fraud prevention and detection, including red flags
- the Code of Conduct, fraud risk program components including and policies.
- policies and procedures, including fraud policy, code of conduct, fraud risk prevention and detection controls, and whistleblower policy, as well as other operational policies such as procurement manuals, etc.

O4.4 Assess Operational Personnel Performance against both role-based performance targets, team or program-based performance targets for which the individual is accountable and other individual performance targets.

P-PROCESS
PO-PLAN & ORGANIZE

PO1-Scope & Objectives

PO1.1 Define Scope of fraud risk management program alone or as part of a broader ethics, compliance and loss prevention program to include preventing, detecting and deterring fraudulent and criminal acts.

PO1.2 Define Stakeholders to include direct internal and external stakeholders of the entity plus the stakeholders relevant to the extended enterprise.

PO1.3 Define Planning Methodology & Team that includes team members with insights into human behavior and higher risk business processes that may prove susceptible to fraudulent behaviors.

PO1.4 Define / Review Organizational Objectives in order to define, align and prioritize fraud risk management initiatives.

PO1.5 Define Program Objectives that measure loss prevention and the protection afforded by detection controls and the prompt resolution of allegations of fraudulent or corrupt conduct.

PO2-Business Model & Context

PO2.1 Identify Key Organizational Entities, Units & Groups as a basis for scoping the program, understanding risks, and prioritizing implementation of fraud risk management program initiatives.

PO2.2 Identify Key Physical, Information and Technology Assets over which or in which specific access, segregation of duty and other fraud prevention and detection controls need to be established.

PO2.3 Identify Key Business Processes that may introduce fraud and corruption risks, including financial, sales and marketing, manufacturing, distribution and fulfillment, research and development and employment.

PO2.4 Identify Key Job Families, Positions, Roles & Assignments including roles in the extended enterprise that are more susceptible to fraud risk due to performance pressures, perceived lack of monitoring, or significant authority over assets, accounts, and disclosures.

PO3-Boundary Identification

PO3.1 Define Boundary Identification Methodology to enable the identification of both mandatory and voluntary boundaries of legal and ethical conduct.

PO3.2 Identify Mandated Boundaries including laws, regulations and treaties proscribing fraud and corruption in all regions of both operation and sales, customary practices in the industry and the geographies and professional conduct standards to which individual in the workforce and/or agents are subject.

PO3.3 Identify Voluntary Boundaries including societal values and norms for the particular industry and geographies of operation and sales relative to fraud and corruption, organizational values to include a commitment to ethical conduct and a no tolerance position on fraudulent, corrupt or illegal behavior.

PO4-Event Identification

PO4.1 Define Event Identification Methodology that includes brainstorming, defines the categories and classifications for various fraud and corruption risks, applies a consistent methodology to facilitate the comparison of risks across business units, departments and groups, includes consideration of unique pressures and business methods in particular industries and geographies that pose greater fraud risk, and past instances of fraudulent or corrupt conduct like management override of controls and the remediation measures already put in place. (See Appendix C and see p. 4 for sources of risk universe information).

PO4.2 Identify and Analyze Events within the organization's culture, product and service mix, processes and systems, trends and changes in the entity's markets, and in society that may introduce specific fraud and corruption related risks like changes in accounting procedures, mergers and consolidation, shifts toward outsourcing or sourcing in areas with weaker detection of risks in the extended enterprise.

PO5-Risk Assessment

PO5.1 Define Risk Assessment Methodology that identifies the frequency of or triggers that require reassessment, utilizes "strategic reasoning" and includes criteria for determining likelihood, impact (monetary, compliance and reputational) and relative priority of risks identified through historical information, known fraud schemes, experience of internal and external audit, subject matter experts for particular geographies and industries, and interviews of business process owners. (See Appendix C).

PO5.2 Analyze Likelihood / Impact in accordance with prescribed methodology and consistently across the enterprise to be able to make meaningful comparison and facilitate prioritization.

PO5.3 Define Priorities to properly allocate available resources to highest priority fraud risks.

PO6-Program Design & Strategy

PO6.1 Define Initiatives to Address Risks whether these are completing initiatives already underway or new initiatives designed to prevent, detect, and mitigate fraud risk based upon an analysis that the initiative is mandated by legal requirements or its projected benefits exceed costs.

PO6.2 Define Initiatives to Address Opportunities & Values to enhance the ethical culture resulting in an environment that is more resistant to fraud risk.

PO6.3 Select Initiatives, Controls & Accountability based upon allocated resource, and relative ranking, identify the particular fraud risk management initiatives and controls that will be pursued, placing them against a portfolio implementation plan and assigning accountability for project management and effectiveness.

PO6.4 Define Crisis Responses to include the scenario where the degree or nature of the fraudulent or corrupt conduct poses catastrophic financial or reputational risk.

PO6.5 Define Strategic Plan in the form substantially like the Fraud Control Strategy or Policy Template that:

- Defines fraud.
- Communicates the entity's commitment to fraud prevention, detection and deterrence.
- Outlines the fraud control strategies, including training and the internal audit strategy relative to fraud control.
- Reflects the fraud control initiatives, including accountability and resources for those initiatives and mitigating resistance to change.
- Reflects the fraud risk management methodology, including identification, assessment and prioritization.
- Documents the fraud roles and responsibilities at all levels of the organization.
- Communicates the procedures for reporting and investigating fraud, including disclosure and discipline.
- Addresses employment considerations, conflict of interest, change challenges and approval.
- Communicates how frequently and by what methods the program will be measured and evaluated.

PR-PREVENT, PROTECT & PREPARE

PR1-General Controls, Policies & Procedures

PR1.1 Develop Controls, Policies & Procedures that represent a mix of controls designed to prevent, detect, monitor, and respond to fraud risk, including:

- Policy defining fraud, irregularities, authority to conduct investigations, confidentiality, and reporting of results of investigations, and potential disciplinary action should fraud be confirmed.
- Policies encouraging high ethical standards and empowering employees, customers and vendors to insist those standards are met.
- Policy that everyone be 100% open and honest with external auditors.
- Policy that fraud involving senior management or that causes a material misstatement of financial statements be reported directly to the audit committee.
- Policy that fraud detected by either internal audit or external audit be brought to the attention of the appropriate level of management.
- Procedures regarding the nature and extent of communications with the audit committee about fraud committed by lower level employees.
- Preventive controls like exit interviews, background checks, training, segregation of duties, performance evaluation, compensation practices, physical and logical access restrictions.
- Detective controls like anonymous reporting, internal audit, and process controls.

PR1.2 Implement and Manage Controls, Policies & Procedures confirming roles and responsibilities related to the fraud policy (See Appendix B), proper communication, implementation of, adherence to, and operation of fraud risk management controls, policies and procedures.

PR1.3 Automate Controls, Policies & Procedures to protect against the risk that fraudulent or corrupt conduct go undetected due to inherent variation in human-centric activities.

PR2-Code Of Conduct

PR2.1 Develop Code of Conduct to include expectations about proper conduct in the face of opportunities for fraud or corruption, non-retaliation for and the proper procedures for reporting identified fraudulent or corrupt conduct regardless of whether the opportunity arises from conflict of interest, use of corporate assets, customer, supplier, government or other business dealings.

PR2.2 Distribute and Manage Code of Conduct publicly and across all levels of the organization so that each level understands and receives training on their respective roles and responsibilities in relation to fraud and corruption risk management, keeping the Code refreshed based upon changes in laws, operating conditions and policies.

PR3-Training & Education

PR3.1 Design / Develop Training related to ethical conduct in the face of stressors or opportunities for fraudulent or corrupt behavior that occur at all levels of the organization and through the extended enterprise, assuring that such training is timely attended based upon changes in roles or responsibilities, and that individuals are meeting comprehension goals.

PR3.2 Implement and Manage Training to confirm that fraud risk management training appropriate to each person's role has been delivered in accordance with the training plan and has met all performance targets.

PR4-Workforce Management

PR4.1 Define Roles, Responsibilities & Duties in relation to fraud risk management responsibilities including segregation of duties and avoidance of conflicts of interest.

PR4.2 Screen & Select Workforce using selection criteria that minimize the risk of future fraudulent conduct based, in part, upon the results of background checks and how the history of any prior inappropriate or unlawful conduct relates to the responsibilities of the position for which the individual is being considered.

PR4.3 Evaluate Performance & Promote Workforce based upon criteria that includes ethical and legal conduct and does not provide incentives or inducements to fraudulent or corrupt conduct.

PR4.4 Compensate & Reward Workforce according to policies and practices that do not provide an incentive or inducement to commit fraud or corruption.

PR4.5 Retire & Terminate Workforce in a manner consistent with fraud policy and using exit interviews as a final confirmation that all organizational assets have been returned, that confidential records have been returned or destroyed in accordance with policy and identifying fraudulent, corrupt or otherwise inappropriate behavior.

PR6-Risk Sharing & Insurance

PR6.1 Design and Implement Risk Sharing & Insurance to protect the entity at an appropriate level based upon the entity's risk tolerance after assessment of residual fraud risk not mitigated by controls, policies, and procedures.

PR7-Preparedness & Practice

PR7.1 Design Preparedness Exercises that afford an opportunity to practice response activities upon the detection of fraud or corruption, including public disclosure and regulatory reporting.

PR7.2 Conduct Preparedness Exercises to determine if planned approaches need to be modified to better protect against fraud risk, particularly reputational risk.

M-ONGOING MONITORING

M1-Control Assurance & Audit

M1.1 Monitor Controls, Policies & Procedures through individuals assigned with such responsibility as periodically reviewed by internal audit, escalating detected issues through appropriate procedures for investigation, response and remediation.

M1.2 Survey Employees and Other Stakeholders as an additional check on whether the anti-fraud program is creating the appropriate culture and is operating effectively, including questions related to whether there has been observed fraudulent or corrupt behavior, whether such was reported, and whether the discipline/response has been consistent, decisive and timely.

M2-Hotline & Helpline

M2.1 Define Hotline/Helpline Approach to consistently address concerns and issues through the validation, investigation, resolution, and remediation processes whether identified through audit or a report of suspected fraudulent or corrupt conduct.

M2.2 Provide Hotline that allows the entity to receive reports of suspected fraudulent or corrupt conduct both on an identified and anonymous basis.

M2.3 Provide Helpline that allows both internal and external stakeholders to obtain guidance on whether observed or suspected conduct constitutes fraudulent or corrupt conduct, and thus should be reported or otherwise addressed in accordance with applicable policies and procedures.

E-PERIODIC EVALUATION

E1-Evaluation Planning & Reporting

E1.1 Define Evaluation Scope / Objectives to include the periodic evaluation of the fraud risk management program.
E1.2 Define Type of Evaluation whether design effectiveness, operating effectiveness and/or performance.
E1.3 Define Level of Assurance and Evaluation Team including whether the evaluation is to be a self-assessment, an internal evaluation with validation or third-party evaluation of the program and/or the quality of internal audit's execution of its role in the program
E1.4 Define Privilege Status for the communications during and results of the evaluation of the fraud risk management program.
E1.5 Develop Evaluation Plan which will vary based upon the defined level of assurance, but must identify the criteria and procedures to be used for assessment in addition to the other elements in the OCEG Foundation. (See Appendices D and E for example self-assessments).
E1.6 Define and Communicate Evaluation Report Content so that the results of the evaluation are communicated at the appropriate level of the organization and ultimately presented by the head of internal audit or the executive-level member of management accountable to the board for the effectiveness and performance of the fraud risk management program as a regular board agenda item.

E2-Program Effectiveness Evaluation

E2.1 Perform Design Effectiveness (DE) Evaluation in accordance with the evaluation plan.
E2.2 Perform Operating Effectiveness (OE) Evaluation in accordance with the evaluation plan.

E3-Program Performance Evaluation

E3.1 Perform Program Efficiency (PE) Evaluation in accordance with the evaluation plan.
E3.2 Perform Program Responsiveness (PR) Evaluation in accordance with the evaluation plan.

R-RESPOND & IMPROVE

R1-Incident, Issue & Case Management

R1.1 Process, Escalate & Manage Incidents in accordance with applicable legal restrictions on anonymous and confidential reporting through a mechanism and process of prompt, competent, and confidential review, investigation, and resolution of allegations involving potential fraud or misconduct which:

- Categorizes issues.
- Confirms the validity of the allegation(s).
- Defines the severity of the allegation(s).
- Escalates the issue or investigation when appropriate.
- Refers issues outside the scope of the program.
- Conducts the investigation and fact-finding.
- Resolves or closes the investigation.
- Undertakes a review of whether the conduct constitutes a control weakness to be remediated.
- Identifies types of information that should be kept confidential.
- Defines how the investigation will be documented.
- Managing and retaining documents and information.

R1.2 Resolve Issues in accordance with the methodology.

R2-Special Investigation

R2.1 Determine Need/Scope of Investigation particularly when the subject of the alleged fraud is based upon conduct of executives or requires specialized skills like forensic accounting.

R2.2 Create Investigation Team to reflect a mix of people with appropriate investigative skills and also knowledge of the business, its procedures, and systems.

R2.3 Plan Investigation consistent with the scope, the policy on investigation procedures and information management plan.

R2.4 Execute Investigation Plan in accordance with the investigation plan.

R2.5 Communicate Investigation/Follow-Up in accordance with the investigation plan, including anonymity, confidentiality and external reporting requirements.

R3-Crisis Response & Communication

R3.1 Execute Crisis and Emergency Response Plan in accordance with the plan, as improved based upon the analysis of lessons learned from practicing the plan and using the designated crisis response team in the various roles identified in the plan.

R4-Discipline & Disclosure

R4.1 Discharge Discipline in accordance with the fraud policy regarding the range of discipline and in conformity to the disciplinary precedents set by prior similar conduct.

R4.2 Disclose Findings to the appropriate level of management, up to and including the board of directors or the audit committee depending on legal requirements and the thresholds set in the escalation policy and as required, to external stakeholders, including the media in accordance with prescribed formats.

R5-Remediation & Improvement

R5.1 Modify Program for Improvement to harden preventive controls, enhance detective controls, and/or accelerate mitigating controls to reduce the risk of loss based upon a reconsideration of how these initiatives rank when compared to the existing portfolio of fraud risk management initiatives.

I-INFORMATION & COMMUNICATION

I1-Information & Records Management

I1.1 Classify Data & Records to facilitate their consistent handling in each of the processes executed as part of the fraud risk management program.

I1.2 Define Information Access based upon each record type in accordance with informational, confidentiality, anonymity, legal and other requirements, and professional standards.

I1.3 Define Information Availability, Integrity & Recovery particularly in the context of transactional history where missing information may be an indicator of the concealment of fraudulent activity.

I1.4 Define Information Management Monitoring particularly related to reports of allegations of fraudulent conduct and to confirm that system overrides or access overrides are authorized and that confidential and other sensitive reports or materials are handled in accordance with stated policy.

I1.5 Define Information Disposition to support the balance of informational needs and the costs of production for investigations or litigation.

I1.6 Define Information Management & Records Awareness Program to make sure those responsible for records related to the fraud risk management program are identifying, managing, handling, and disposing of records according to the stated policies and procedures.

I2-Communication

I2.1 Develop Communication Plan for fraud related policies, procedures, training, investigations, and reporting.

I2.2 Deliver Communications in accordance with the communication plan(s).

I3-Internal Reporting

I3.1 Develop Internal Reports that reflect risk analysis, prioritized portfolio of risk initiatives, progress toward fraud risk management objectives, the status and results of evaluations, and the status, results and discipline taken in response to investigations.

I3.2 Develop Internal Communications

I4-External Reporting & Filings

I4.1 Develop Disclosure Systems and Forms that comply with information management and crisis response procedures and meet the informational needs and requirements of the organization and the external party, complying with submission on any mandated reporting forms.

I4.2 Create and Manage Disclosures & Filings in accordance with the defined procedures and forms.

T-TECHNOLOGY

T1-Technology

T1.1 Leverage Technology to Support Program particularly with regard to:

- automating controls that monitoring transactions, enforce business rules, and segregation of duties.
- sharing knowledge of trends and history of incidents, risks, and discipline to facilitate risk analysis and disciplinary decisions.
- enabling reporting of alleged fraud or corruption.
- incident management and loss tracking.
- forensic investigations.

APPENDIX I: COSO INTERNAL CONTROL INTEGRATED FRAMEWORK

COSO Component	Fraud Risk Management Activities
Control Environment	• Establishing appropriate "tone at the top" and organizational culture. • Documenting fraud control strategy, code of ethics/conduct, and hiring and promotion standards. • Establishing, complementing, or evaluating internal audit functions. • Developing curriculum; designing and providing training. • Developing a policy and methodology to investigate potential occurrences of fraud. • Investigating allegations or suspicions of fraud. • Promoting controls to prevent, deter, and detect fraud. • Implementing and maintaining a fraud and ethics hotline and whistleblower program.
Fraud Risk Assessment	• Establishing a fraud risk assessment process that considers fraud risk factors and fraud schemes. • Involving appropriate personnel in the fraud risk assessment process. • Performing fraud risk assessments on a regular basis.
Anti-fraud Control Activities	• Defining and documenting mitigating controls and linking them to identified fraud risks. • Modifying existing controls, designing and implementing new preventive and detective controls as necessary, and implementing supporting technologies.
Information and Communication	• Promoting the importance of the fraud risk management program and the organization's position on fraud risk both internally and externally through corporate communications programs. • Designing and delivering fraud awareness training.
Monitor	• Providing periodic evaluation of anti-fraud controls. • Using independent evaluations of the fraud risk management program by internal auditing or other groups. • Implementing technology to aid in continuous monitoring and detection activities.