



November 13, 2007

Dear Colleague,

On behalf of the Association of Certified Fraud Examiners, The American Institute of Certified Public Accountants, and The Institute of Internal Auditors, I am pleased to present to you the attached exposure draft of “Managing the Business Risk of Fraud: A Practical Guide”. This paper was prepared to provide a summary resource for organizations to use in considering their exposures to fraud risks and the appropriate reaction to those risks. This work is the result of a task force of over 20 experts in the field of fraud risk identification, mitigation, and investigation.

The paper offers guidance to the principles, practices, and benefits of an antifraud program for organizations committed to preserving stakeholder value. It can be used to assess an organization’s antifraud program, as a resource for improvement, or to develop an antifraud program where none exists. The document contains five key principles of a fraud risk management process. Each of these principles is explained in the paper. In addition, appendices are included to provide references to other key documents on this topic (with web addresses where possible), plus several examples and tools which you can use in determining your organization’s approach to fraud risk management.

The exposure draft will remain available for comments from November 13, 2007 through December 21, 2007. Your comments and suggestions can be sent via e-mail to: www.fraudguidance@theiia.org.

This document is being circulated to a number of organizations and key leaders in the regulatory and guidance issuing areas. It is our expectation that inputs received will be consolidated and a final version of the document will be available in January 2008.

A shorter “Executive Summary” document will be included with the final paper which will be made available specifically for board members, audit committee chairs, senior executive management, and others to provide a high level overview of this topic.

Please feel free to submit your comments by referring to specific pages and paragraphs in the document or providing general overall comments about the content and usefulness of the document. We look forward to hearing from you.

Sincerely,

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

Managing the Business Risk of Fraud: A Practical Guide

EXPOSURE DRAFT
November 12, 2007

Sponsored by:
The Association of Certified Fraud Examiners
The American Institute of Certified Public Accountants
The Institute of Internal Auditors

Managing the Business Risk of Fraud: A Practical Guide

DRAFT 11/12/07

<u>TABLE OF CONTENTS</u>	<u>PAGE</u>
SECTION 1: INTRODUCTION.....	3
SECTION 2: FRAUD RISK GOVERNANCE.....	8
SECTION 3: FRAUD RISK ASSESSMENT.....	16
SECTION 4: FRAUD PREVENTION.....	25
SECTION 5: FRAUD DETECTION.....	29
SECTION 6: INVESTIGATION AND RESPONSE.....	35
SECTION 7: CONCLUDING COMMENTS.....	40
APPENDICES:	
APPENDIX A: REFERENCE MATERIAL	41
APPENDIX B1: FRAUD GOVERNANCE POLICY CONTENT.....	44
APPENDIX B2: SAMPLE FRAUD POLICY.....	46
APPENDIX C1: FRAUD RISK ASSESSMENT FRAMEWORK EXAMPLE	51
APPENDIX C2: FRAUD RISK EXPOSURES.....	53
APPENDIX D: FRAUD PREVENTION SCORECARD.....	57
APPENDIX E: FRAUD DETECTION SCORECARD.....	61
APPENDIX F: ALIGNMENT OF PRINCIPLES TO OCEG FOUNDATION.....	65
APPENDIX G: COSO FRAUD RISK MANAGEMENT ACTIVITIES.....	74

Managing the Business Risk of Fraud: A Practical Guide

Fraud is any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and/or the perpetrator achieving a gain.

SECTION 1: INTRODUCTION¹

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. Regulations such as the 1977 U.S. Foreign Corrupt Practices Act, the 1997 Organization for Economic Co-operation and Development Anti-Bribery Convention, the U.S. Sarbanes-Oxley Act of 2002, and the 2005 U.S. Federal Sentencing Guidelines have increased the responsibility to deter, prevent, and detect fraud.

Managing fraud risk has taken on a higher profile since the enactment of the Sarbanes-Oxley Act and similar legislation throughout the world. Scandals occurring in the past few years have emphasized overall public and organization stakeholder expectations for a “no fraud tolerance” attitude. Impacts on the reputation, brand, and image of organizations have resulted from publicized fraudulent behavior of key executives in many global organizations. Good governance principles demand that the board ensure overall high ethical behavior by management of any organization regardless of its status as public, private, government, or not-for-profit, or its relative size or industry. The board’s role is critically important because historical records indicate that most major frauds are perpetrated by senior management in collusion with other employees². Handling of fraud cases within an organization sends clear signals to regulators and stakeholders about the board and management’s attitude toward fraud risks and about how the organization’s policies are implemented.

A 2007 Oversight Systems study³ discovered that the primary reasons why frauds occur are “pressures to do ‘whatever it takes’ to meet goals” (81 percent of respondents) and “seek personal gain” (72 percent), while 40 percent indicated that “they do not consider their actions fraudulent” also was a reason for wrongful behavior.

The board, management, employees, and internal auditing all have responsibility for managing fraud risk. Fraud has serious repercussions on organizations in areas such as reputation, product quality/safety, employee health, and sale of customer information. Due to the heightened regulatory environment, as well as increased public attention, boards of directors, executive management, and internal auditors, among others, are being asked specifically how the organization is responding to these regulations, how they identify fraud risks, what they are

¹ “Antifraud program” refers to the process used within an organization to address potential and actual fraud occurrences. The form, documentation, and content will vary depending on the size, complexity, and overall structure of the organization. This definition of fraud was developed uniquely for this paper, and the authors recognize that many other definitions of fraud exist.

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

³ Per the 2007 Oversight Systems Report on Corporate Fraud (www.oversightsystems.com).

doing to better prevent or at least detect fraud sooner, and what programs and procedures are in place to investigate fraud.⁴ This document is designed to help address these tough issues.

Executive Summary

Fraud is any intentional act or omission designed to deceive others and resulting in the victim suffering a loss and/or the perpetrator achieving a gain. Fraud can be categorized into fraudulent financial reporting, misappropriation of assets, and improper or unauthorized expenditures. Regardless of culture, ethnicity, religion, or other factors, certain individuals will be motivated to commit fraud. Only through diligent and constant effort can an organization protect itself against significant acts of fraud.

The following principles outline the key steps for proactively establishing an environment to manage fraud risk in an organization effectively:

Principle 1: A fraud risk policy should be written to convey to the organization the expectations of the board of directors and executive management regarding managing fraud risks.

Principle 2: Fraud risk exposure should be assessed by the organization to identify specific potential 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 potential impacts on the organization.

Principle 4: Detection methods 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 inputs on potential fraud events and a coordinated investigation approach should be used to ensure potential fraud events are dealt with in a timely manner.

The following is a summary of the paper prepared to provide a practical guide to the principles, practices, and benefits of an antifraud program for organizations committed to preserving stakeholder value. This guide can be used to assess an organization's antifraud program, as a resource for improvement, or to develop an antifraud program where none exists.

Fraud Risk Governance Process

Organization stakeholders have clearly raised expectations for ethical organizational behavior. Regulators worldwide have increased criminal penalties that can be levied against organizations and individuals who participate in committing fraud. Organizations should respond to such expectations. Effective governance processes are the foundation for preventing, detecting, and

⁴ See 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 Oversight Board (PCAOB) Auditing Standard No. 5 (AS5), An Audit of Internal Controls Over Financial Reporting That Is Integrated With an Audit of Financial Statements, for comments on fraud responsibilities.

detering fraudulent acts. Lack of effective governance processes seriously undermines any antifraud programs, policies, procedures, and controls. Enforced human resource (HR) policies and the organization's overall tone at the top set the standard regarding its tolerance of fraud.

The board of directors should ensure its own governance practices set the tone for fraud prevention and that management implements policies that encourage ethical behavior, and provide processes for employees, customers, and vendors to report instances where those standards are not met. It should monitor the fraud risk governance program's effectiveness, which should be a regular agenda item at periodic meetings. The board should appoint one executive-level member of management to be responsible for fraud risk governance programs and reporting to the board on the topic.

Governance policies should provide for the design and implementation of a comprehensive and coordinated approach to fraud mitigation. A fraud mitigation strategy or equivalent should cover:

- The board's and the organization's commitment to fraud prevention, detection, and deterrence.
- Fraud awareness training.
- Roles and responsibilities.
- Conflict of interest disclosure process.
- Periodic affirmation process.
- Fraud risk assessment and control planning.
- Reporting procedures.
- Investigation and discipline.

Fraud Risk Assessment

To effectively and efficiently protect itself and its stakeholders 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 part of an overall organizational risk assessment or a stand-alone exercise, but should include risk identification, identified risk likelihood and significance assessment, and risk response.

Fraud risk identification may include gathering external information from industry sources and U.S. Securities and Exchange Commission (SEC) enforcement actions, litigation, and settlements, as well as from organizations such as the American Institute of Certified Public Accountants (AICPA), The Institute of Internal Auditors (IIA), the Association of Certified Fraud Examiners (ACFE), the Canadian Institute of Chartered Accountants, and the American Bar Association. Case law, surveys, or guidance from similar organizations within a specific country (e.g., Cadbury, King Report) can also be useful. Internal sources for identifying fraud risks should include interviews and brainstorming with personnel representing a broad spectrum of activities within your 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 reputation and its legal and regulatory compliance requirements. An initial assessment of fraud risk should consider the inherent risk of a particular fraud in the absence of any known controls that may address the risk. An organization can cost-effectively manage its fraud risks by assessing the likelihood and significance of fraudulent behavior.

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 antifraud controls program provides should exceed its cost. 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 shareholders, members, donors, citizens, etc., depending on organizational form. These controls should be designed appropriately and executed efficiently by competent and objective individuals.

Fraud Prevention, Detection, and Deterrence

Fraud prevention and detection are related, but are not the same concepts. Prevention focuses on policies, procedures, training, and communication that stop fraud from occurring, whereas detection focuses on activities and programs that recognize timely whether fraud has occurred or is occurring. While preventive measures do not ensure fraud will not be committed, they are the first line of defense in minimizing fraud risk.

One key to prevention is expanding from the board down throughout the organization an awareness of the types of fraud that may occur as well as awareness of the antifraud program. HR activities such as background investigations, new hire training on governance processes, effective performance evaluation and compensation practices, and exit interviews are important preventive/detective measures. Additional preventive controls include restricting physical and logical access to designated individuals, appropriate authorization and approvals, and ensuring adequate segregation of duties.

One of the strongest fraud deterrents is the perception that effective detective controls are in place. Combined with preventive controls, detective controls enhance the effectiveness of an antifraud program by showing that preventive controls are working as intended and identifying fraud if it occurs. Although detective controls may provide evidence that fraud has occurred or is occurring, they are not intended to prevent fraud. Significant fraud risk areas should have controls in place specifically designed to prevent fraud in those areas.

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 if the estimated impact of the scheme exceeds the cost of the control, including tools, personnel, and training. Three important fraud-detection methods are an anonymous reporting mechanism to the board (e.g., hotline), internal auditing, and process-related controls specifically designed to detect fraudulent activity.

Fraud Investigation and Response

No system of internal control can provide absolute assurance against fraud. The board should define its own role in investigation processes and should ensure the organization develops a system for prompt, competent, and confidential review, investigation, and resolution of allegations involving potential fraud. An organization can improve its chances of loss recovery, while minimizing exposure to litigation and damage to reputation by establishing and preplanning investigation and response processes. The board is responsible for ensuring that these measures are in place.

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, the board should ensure that its role in investigations is clearly defined and that the organization has an appropriate and effective process to investigate cases. A consistent process for conducting investigations can help the organization mitigate losses and manage risk associated with the investigation. Consistent 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 need to be made for investors, shareholders, or the media.

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 a sufficient basis for those actions. Actions taken should be appropriate under the circumstances, applied consistently to all levels of employees, including top management, and taken only after consultation with individuals responsible for such decisions. Consulting legal counsel is strongly recommended before undertaking an investigation and is critical before taking disciplinary, civil, or criminal action.

Thus, to properly address fraud risk within the organization, the following key steps are needed to ensure:

- A suitable oversight process exists (governance).
- Fraud exposures are identified (risk assessment).
- Appropriate programs and procedures are in place to manage these exposures (prevention, detection and deterrence).
- Reaction to fraud allegations are addressed in a timely manner (investigation).
- The facts surrounding allegations of fraud, as well as how such allegations were handled, are captured for review (response).

SECTION 2: FRAUD RISK GOVERNANCE

Principle 1: A fraud risk policy should be written to convey to the organization the expectations of the board of directors and executive management regarding managing fraud risks.

Corporate governance has been defined in many ways, including “The system by which companies are directed and controlled” (Sir Adrian Cadbury, The Committee on the Financial Aspects of Corporate Governance), and “The process by which corporations are made responsive to the rights and wishes of stakeholders” (Ada Demb and F. Friedrich Neubauer, *The Corporate Board: Confronting the Paradoxes*). 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 (i.e., shareholders, employees, customers, vendors, governmental entities, community organizations, and the media) have raised the awareness and expectation for ethical 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 the whistleblower hotline.
- Independent nomination processes.
- Effective senior management team evaluations (including chief executive officer (CEO), chief financial officer, and chief operating officer), performance management, compensation, and succession planning.
- 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, promotion, and remuneration policies for employees, as well as ethics considerations in all aspects of their relationships with customers, vendors, and other corporate stakeholders. Effective boards and organizations will also 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 objectives varies widely and directly affects the fraud risk profile of an organization.

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 amounts⁵. 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 and corruption. In many organizations this is managed as part of corporate governance through entity-level controls, including ethics, compliance, and fraud risk management programs.

It is important to recognize that ethics goes beyond mere compliance programs to include corporate culture; when entities make ethics a priority the benefits outweigh the costs. For instance, effective business ethics programs can serve as the foundation for preventing, detecting, and deterring fraudulent and criminal acts. These ethics programs create an environment where making the right decision is implicit, whereas compliance programs focus on preventing wrong decisions that can lead to legal and regulatory violations. Both are important foundational components to effective fraud risk management. To this end, not only is ethics and compliance important, but inclusion of fraud risk management is also key to corporate governance.

Roles and Responsibilities

Personnel at all levels of the organization have roles and responsibilities with respect to fraud prevention, detection, and deterrence. These responsibilities, at minimum, should be formally documented as part of the 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, and audit committees.

The board has the responsibility to 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 every day. The board should:

- Have a thorough understanding of what constitutes fraud and corruption risk.
- Set the appropriate tone at the top in its own independent practices and through the CEO job description, evaluation, and succession-planning processes.
- Maintain oversight of the fraud risk assessment.

⁵ 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.

- Evaluate management's identification of fraud risks.
- Oversee the internal controls over financial reporting established by management.
- Assess the risk of financial fraud by management.
- Ensure controls are in place to prevent, deter, and detect fraud by management.
- Empower a committee of the board (usually the audit committee) and external auditors to look for and report fraud.

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 these objectives.

The board should also 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. In its communications with relevant parties, the board should assess the degree to which these parties believe the organization's fraud practices and policies are adequate.

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 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.

The board is also responsible for monitoring the effectiveness of the programs, a responsibility that should be addressed under a periodic agenda item at board meetings when general risks of the organization are considered.

Audit Committee

An audit committee of the board, or similar oversight body, that is committed to a proactive approach to fraud risk management plays an active role in the risk assessment process, and uses the internal audit department, and perhaps the external auditors, to monitor fraud risks. *Management Override of Internal Controls: The Achilles' Heel of Fraud Prevention*, an AICPA publication, provides valuable information for audit committees taking this approach.

The audit committee should be aware that the entity's external auditors have a responsibility to plan and perform the audit of the entity's financial statements to obtain reasonable assurance about whether the financial statements are free of material misstatement caused by fraud. The external auditor, as part of the audit, among other things:

- a) Considers events or conditions that indicate incentives/pressures to perpetrate fraud, opportunities to carry out the fraud, or attitudes/rationalizations to justify a fraudulent action.

- b) Brainstorms among the audit team members about how and where they believe the entity's financial statements might be susceptible to material misstatement due to fraud.
- c) Inquires of management and others within the entity about the risks of fraud.
- d) Performs analytical procedures to identify unusual transactions or events, and amounts, ratios, and trends that might indicate matters that have financial statement implications.

The audit committee should insist on openness and honesty with the external auditors. The external auditors should also have the commitment and cooperation of the audit committee.

Additionally, whenever the external auditor has determined that there is evidence that fraud may exist, the external auditor's professional standards state that the matter should be brought to the attention of an appropriate level of management. That is appropriate even if the matter might be considered inconsequential, such as a minor defalcation by an employee at a low level in the entity's organization. The audit committee should reach an understanding with the external auditor regarding the nature and extent of communications with the committee about fraud committed by lower-level employees. In addition, the external auditor's professional standards state that the auditor should report fraud involving senior management and fraud — whether caused by senior management or other employees — that causes a material misstatement of the financial statements directly to the audit committee.

The audit committee should also seek the advice of counsel whenever dealing with issues of allegations of fraud. Because fraud allegations are serious, there may be a legal duty to investigate and/or report them.

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 control. At each meeting the audit committee should meet separately with the external audit firm and the chief internal audit executive to express its expectation that their work focus significantly on detecting any material fraud that has a direct impact on the organization's finances. In addition, since reputation risk resulting from fraudulent behavior often has a severe impact on shareholder value, the audit committee should provide specific consideration and oversight of this exposure when reviewing the work of management, internal auditors and external auditors.

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. 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.

In meeting its responsibilities, management needs to report to the board regularly on the effectiveness of the program and any remedial steps that are needed.

Staff

Strong controls against fraud are the responsibility of everyone in the organization, including staff. Staff and management should:

- Understand their role within the internal control framework.
- Read and understand policies and procedures, including fraud policy, code of conduct, and whistleblower policy, as well as other operational policies such as procurement manuals.
- As required, participate in the process of creating a strong control environment and designing and implementing control activities, as well as participate in monitoring activities.
- Report incidences of fraud.
- Have a basic understanding of fraud and corruption and be aware of the red flags.

Internal Auditing

Internal auditing should provide assurance that fraud prevention and detection controls are sufficient for identified fraud risks, and ensure that the controls are functioning as designed. Internal auditing should also be alert for incidences of actual fraudulent activity and may be responsible for initial or full investigation of suspected fraud schemes.

Fraud Risk Management Program

Formal documents should provide for the design and implementation of a comprehensive and coordinated approach to fraud control. While most organizations have rules relating to theft, fraud, and corruption in their code of conduct, not all have outlined the complete range of subjects necessary for an effective fraud risk management program.

The importance of internal controls in the prevention, detection, and deterrence of fraud is not a new concept. In 1992, after more than three years of collaboration between corporate leaders, legislators, regulators, auditors, academics, and many others, The Committee of Sponsoring Organizations of the Treadway Commission (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 will simply not be tolerated at any level. Appendix F suggests activities aligned with each COSO component.

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

- A single comprehensive and complete document addressing in detail all aspects of fraud controls.
- 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.
- A compilation of plans developed by divisions or subsidiaries.

While each organization needs to consider its size and complexity when determining what type of formal documentation is most appropriate, best practice is to have a formal fraud control policy⁶ that discusses practices that fall into each of the COSO elements. The document should at least reference the elements detailed below.

The Organization's Commitment to Fraud Prevention, Detection, and Deterrence

The board of directors and management should summarize their commitment to a fraud risk management program in 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 prevention, detection, and deterrence activities. The letter should be endorsed or authored by a senior executive or board member and reissued periodically.

This statement of the organization's commitment should provide a framework and awareness of the organization's fraud risk strategy. The letter should also serve as the foundation for and may be the executive summary of the fraud control policy.

The Elements of an Effective Policy on Fraud and Availability of Fraud Awareness Training

The policy should define fraud, including the risk of fraudulent financial reporting, misappropriation of assets, and corruption. The policy and training should identify potential perpetrators of fraud, provide examples of the types of fraud that could occur, and raise awareness that fraud may be perpetrated by internal parties, external parties, or collusively. Considering that people commit fraud and that people are an organization's best asset in preventing, detecting, and deterring fraud, a best practice would be to make a reference to available fraud reporting resources that individuals may access, such as via the organization's Web site or whistleblower hotline (also see reporting procedures below).

The Roles and Responsibilities for Fraud Prevention, Detection, and Deterrence

This section of the policy should define roles and responsibilities related to the fraud risk management program. The policy should start by articulating the governance oversight of fraud control (i.e., the role and responsibility of the board of directors/audit committee) as reflected in the board and audit committee charters.

⁶ Refer to the sample fraud control policy outline in Appendix B2.

The policy also should reflect management's responsibility for the design and implementation of the fraud control strategy, and how different segments of the organization support the fraud risk management program. For instance, HR may provide fraud awareness training and be responsible for the whistleblower hotline. Often the fraud risk management program will be supported by not only HR but also risk management, compliance, general counsel, the ethics office, security, information technology (IT), and internal auditing, or their equivalents.

To this end, the policy should reflect the role of internal auditing or its equivalent in monitoring the effectiveness and efficiency of the fraud risk management program. These monitoring efforts should be consistent with the guidance provided in IIA Practice Advisory 1210.A2-1: Auditor's Responsibilities Relating to Fraud Risk Assessment, Prevention, and Detection.

Most importantly, the policy should articulate the responsibility of employees in helping to prevent, detect, and deter fraud.

Conflicts of Interests\Code of Conduct or Other Ethics and Compliance Policies

Many organizations have existing policies, procedures, and forms that support a comprehensive fraud risk management program. Within the policy document, reference should be made to policies that support the prevention, detection, and deterrence of fraud. For instance, reference to the code of conduct and policies regarding conflicts of interest often support the overall fraud risk management program.

Affirmation Process

An affirmation of the policy should describe the requirement for directors, employees, and contractors to acknowledge they have read, understood, and complied with the code of conduct and/or the fraud control policy. This 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.

Disclosure Process

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

- Management may assert that there is a conflict and require the individual to terminate the activity or leave the organization.
- Management may accept the 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 should be documented⁷. Any constraints placed on the situation need to be monitored. For example, a buyer who has 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 control policy.

Fraud Risk Assessment and Control Planning

The foundations of an effective fraud risk management program are rooted in a risk assessment that identifies where fraud may occur within the organization. A fraud risk assessment should be required by the board and the board should oversee that risk assessment process.

The fraud risk assessment should be performed on a systematic and recurring basis, involving appropriate personnel, considering relevant fraud schemes and scenarios, and mapping those fraud schemes and scenarios to mitigating controls. The policy should reflect consideration of both preventive and detective controls in mitigating fraud risk. The existence of the fraud risk assessment and the fact that management is articulating its existence may deter would-be fraudsters.

Reporting Procedures

The fraud risk policy should articulate the organization's zero tolerance for fraud and establish the expectation that suspected fraud should be reported immediately. The channels to report suspected fraud issues should be clearly defined and may be the same or different for other code of conduct violations. 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.

Investigation Process

The fraud risk policy 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, rules of evidence, chains of custody, reporting mechanisms to those charged with governance, regulatory requirements, and legal actions.

⁷ Waivers of provisions of conflicts of interest policies 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.

Discipline and Remediation

As a deterrent, the policy should reflect the consequences for fraudulent activity. These consequences may include termination of employment or of a contract and reporting to legal and regulatory authorities.

When fraud does occur within the organization, the policy should reflect the need to conduct a postmortem to identify the control weakness that failed to prevent the fraudulent act. The postmortem should lead to a remediation of any identified control deficiencies.

The organization should articulate that it has the right to institute civil or criminal action against anyone who commits fraud.

Process Evaluation and Improvement (Quality Assurance)

The policy should describe whether, 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 results⁸. The results of this evaluation should be reported to appropriate oversight groups and be used by management to improve the program.

Maintenance

The fraud risk document should be revised and reviewed based on the changing needs of the organization, recognizing that it is not a static document. The document should be maintained, updated, and improved to reflect the organization's commitment to fraud prevention, detection, and deterrence.

SECTION 3: FRAUD RISK ASSESSMENT

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

Regulators, professional standard-setters, and law enforcement authorities have emphasized the crucial role fraud risk assessment plays in developing and maintaining effective antifraud programs and controls.⁹ Organizations can identify and assess fraud and misconduct risks in conjunction with an overall enterprise risk assessment or on a stand-alone basis.

This section provides a practical guide for conducting a fraud risk assessment. Organizations can tailor this approach to meet their individual needs, complexities, and goals.

⁸ Refer to a more complete list of potential statistics, benchmarks, and other comparisons in Appendix F.

⁹ June 2007 SEC Guidance to Management; PCAOB AS5; IIA Practice Advisory 1210-A2-1: Auditor Responsibilities Related to Fraud Risk Assessment, Prevention, and Detection; *COSO for Small Business*: Principle 10–Fraud Risk; Statement of Auditing Standards (SAS) No. 99, Consideration of Fraud in A Financial Statement Audit; and International Standards on Auditing (ISA) No. 240.

Fraud, by definition, entails intentional misconduct, designed to evade detection. As such, the fraud risk assessment team should engage in strategic reasoning to predict the behavior of a potential fraud perpetrator.¹⁰ Strategic reasoning requires a skeptical mind-set and involves asking questions such as:

- How might a fraud perpetrator exploit weaknesses in the system of controls?
- How could a perpetrator override or circumvent controls?
- What could a perpetrator do to conceal the risk of fraud?

Strategic reasoning is also important in designing fraud-detection procedures that a perpetrator may not anticipate.

A fraud and misconduct risk assessment generally includes three elements:

- *Identify inherent fraud risk*¹¹ — Gathering information to obtain the population of fraud risks that could apply to your organization. Included in this process is the explicit consideration of all types of fraud; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to your organization.
- *Assess likelihood and significance of inherent fraud risk* — Assessing the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with business process owners.
- *Respond to reasonably likely and significant inherent and residual fraud risks* — Deciding what the response should be to address the identified risks; performing a cost-benefit analysis of fraud risks over which the organization wants to implement controls or specific fraud-detection procedures.

Organizations should apply a framework to document their fraud risk assessment, beginning with a list of identified fraud schemes, which are then assessed for relative significance and likelihood of occurrence. The team should then map the risks to relevant controls, which are evaluated for design effectiveness and tested to validate operating effectiveness. Next, the organization should develop a response to residual fraud risks. The following framework illustrates how the elements of fraud risk identification, assessment, and response are applied in a rational, structured approach.

¹⁰ 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).

¹¹ 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.

Fraud Risks Identified	Likelihood	Significance	People and/or Department	Antifraud Controls	Assess Effectiveness Of Controls	Residual Risks	Fraud Risk Response
<p><i>Financial reporting</i></p> <ul style="list-style-type: none"> Revenue recognition <ul style="list-style-type: none"> - Backdating agreements - Channel stuffing - Holding books open - Additional revenue risks Management estimates <ul style="list-style-type: none"> - Self insurance - Allowance for bad debts - Additional estimates Disclosures <ul style="list-style-type: none"> - Footnotes - Additional disclosures <p><i>Misappropriation of assets</i></p> <ul style="list-style-type: none"> - Cash/check <ul style="list-style-type: none"> - Point of sale - Accounts receivable application process - Master vendor file controls override - Additional risks - Inventory <ul style="list-style-type: none"> - Theft by customers - Theft by employees - Other assets at risk <p><i>Corruption</i></p> <ul style="list-style-type: none"> - Bribery - Aiding and abetting - Other risks 							

Assembling the Risk Assessment Team

A fraud risk assessment team should include individuals from throughout the organization with different knowledge, skills, and perspectives. The team should include a combination of internal and external resources:

- 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 enterprise risk management program.
- Legal and compliance personnel, as the fraud and misconduct 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.
- External consultants with expertise in applicable standards, key risk indicators, antifraud methodology, control activities, and detection procedures.

Senior management, business unit leaders, and significant process owners should participate in the assessment, as they are ultimately accountable for the effectiveness of the organization’s antifraud efforts.

Fraud Risk Identification

Brainstorming

An effective risk identification process includes brainstorming about fraud risks by personnel representing a broad spectrum of activities within the organization (e.g., accounting, management, sales, procurement, and operations). 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 controls¹². Brainstorming should include discussion 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.

The team should share this information and solicit comments from the board or audit committee. In addition, the board should also assess the implications of its own processes with respect to its contribution to fraud risk and incentive pressures.

Incentives, Pressures, and Opportunities

The fraud risk identification process includes an assessment of the incentives, pressures, and opportunities to commit fraud. Incentive programs should be evaluated — by the board for senior executives 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 can 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. Maintaining the status quo is sometimes a powerful enough incentive for personnel to commit fraud. This is why analytics alone are generally not a good method of detecting fraud, as fraudulent adjustments are often recorded to make the analytics look “right.”

¹² 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.”

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 enough pressure — real or perceived — on an employee to act fraudulently. Are the pressures at your organization such that someone might record an adjustment in order to make budget?

Opportunities to commit fraud exist throughout organizations. 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. This is why appropriate monitoring of top management by a strong board and audit committee, supported by internal auditing, is critical to preventing and detecting fraud.

Risk of Management's Override of Controls

As part of the risk identification process, it is important to consider the potential override of controls. The team should also consider the risk of management override when evaluating the effectiveness of controls; an antifraud control is not effective if it is easily overridden.

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.

Population of Fraud Risks

The fraud risk identification process requires an understanding of the universe of fraud risks and the subset of risks that apply to an organization. This phase includes obtaining information from external sources, such as industry news, criminal, civil, and regulatory complaints and settlements, as well as from organizations such as the ACFE and The IIA. The risk identification process will also include gathering information about potential fraudulent acts from internal sources by interviewing personnel; understanding business processes; conducting brainstorming sessions; understanding incentives, pressures, and opportunities to commit fraud in the organization; reviewing complaints on the whistleblower hotline; and performing analytical procedures.

Various taxonomies are available to organize fraud and misconduct risks. The ACFE, for example, classifies fraud risks into three general categories: fraudulent statements, misappropriation of assets, and corruption. Using this as a starting point, a more detailed breakout can be developed to produce an organization-specific fraud risk assessment.

- 1) Intentional manipulation of financial statements 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 category in the previous section 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 financial reporting schemes are common across all organizations (e.g., “cookie jar” reserves 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 on page 17 and in Appendix C1 to identify specific areas of greatest risk. Using this framework as a foundation, organizations can customize the assessment process for their specific needs. For example, starting with the revenue recognition component of fraudulent financial reporting, the assessment should consider:

- What are the main drivers of revenue at your 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 your organization?
- Are revenues recorded systematically or manually?

- Are there any revenue recognition fraud risks specific to your industry?

Or, consider significant marketplace disclosures (e.g., loan delinquency percentages):

- What controls are in place to monitor your internal gathering and reporting of these disclosures?
- Is there oversight from someone whose compensation is not directly affected by his or her “success”?
- Does someone monitor your organization’s disclosures in relation to other organizations and ask hard questions about whether your organization’s disclosures are adequate or could be improved?

The categories of fraudulent financial reporting shown in the previous section 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.

Motives 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.

There is a fourth category, 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 includes not only the theft or misuse of assets, but also improper financial reporting.

Misappropriation of Assets

Assets, both tangible and intangible, can be stolen by employees, customers, or vendors. The organization should ensure that controls are in place to protect them. Common schemes include misappropriation by:

- Employees by establishing fictitious vendors.
- Employees of customer or other sensitive data.
- Employees by theft of physical assets (e.g., inventory, portable fixed assets).
- Employees in collaboration with vendors or customers.
- Employees through expense reporting abuse.
- Ex-employees, and others outside the organization, of sensitive or other significant information.
- Vendors by intentional over billing.
- Customers by theft of inventory.
- Customers by fraudulent credit transactions.

Protecting against these risks requires not only physical safeguarding controls, but also periodic detective controls such as physical counts and reconciliations to the general ledger. Remember, a smart perpetrator may be thinking about such controls and design the fraud to be concealed from those controls. Considerations to be made in the risk assessment process include gaining an understanding of what assets are subject to theft, in how many locations the assets are maintained, how many personnel have the ability to approve new vendors or issue disbursements, and how many personnel have access to tangible or intangible assets.

Corruption

Corruption is operationally defined as the misuse of entrusted power for private gain. The U.S. Foreign Corrupt Practices Act (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. Organizations that have operations outside the United States need to consider the FCPA requirements in their antifraud program.

Other Risks

Aiding and Abetting — Law enforcement authorities worldwide have prosecuted numerous cases where companies 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 in your organization may be engaging in such behavior.

Other Regulatory and Legal Misconduct — This category includes a wide range of types of misconduct risk, 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 your 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 risk managers, 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 that could increase the organization's cost of borrowing and depress its market capitalization. Because boards are responsible for the longevity of the organization and have responsibilities to multiple stakeholders, the board should regularly evaluate its performance with respect to reputation risks.

Information Technology 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 a variety of threats that can result in significant financial and information losses and an ongoing threat of

cyber fraud. 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, unauthorized access to data, cyber fraud can affect everyone. 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, 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.

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 both know its vulnerabilities and be able to mitigate risk in a cost-effective manner. Therefore, an IT risk assessment should be incorporated into an organization's overall fraud risk assessment.

Assessment of the Likelihood and Significance of Identified Inherent 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 your organization. Assessing likelihood and significance allows the organization to manage its fraud risks and apply preventive and detective procedures rationally.

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, the organization's overall control environment, 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 frauds occurring in as many buckets as deemed reasonable, but three categories are generally adequate: remote, reasonably possible, and probable.

Significance — The 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, significant, 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 Reasonably Likely and Significant Inherent and 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.

Frauds 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 fraud 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, you are looking at your organization's financial statements and operations

and asking “What can be wrong in this picture?”, and then designing appropriate controls. The key is to be selective and efficient. There are probably thousands of potential controls that could be put in place. What you want is a targeted and structured approach, not an unstructured or haphazard approach. You also want efficient controls that deliver the most for the resources they will cost. The objective is to have the benefit of controls exceed their cost.

In addressing fraud risks, one should be careful to ensure that controls that are identified as antifraud 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 antifraud control would include an evaluation of the underlying support for consistency in application from prior periods and for potential inappropriate bias. Therefore, antifraud controls should be designed appropriately and executed by competent and objective individuals. Management’s documentation of antifraud controls should include the description of what the control is designed to do, who is to perform the control, and the related segregation of duties.

The design of antifraud controls and fraud auditing procedures are addressed in the next two sections of this paper: fraud prevention and detection.

SECTION 4: FRAUD PREVENTION

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

The governance process plays a key role in an organization’s antifraud program. Yet despite the best efforts of boards of directors, chief risk officers, internal auditors, and others who are responsible for preventing fraud, one inevitable reality remains: “fraud happens.” Because fraud and misconduct can occur at various levels in every organization, it is essential that appropriate preventive and detective mechanisms are in place. Fraud prevention and detection are related, but are not the same concepts. Prevention focuses on policies, procedures, training, and communication, whereas detection focuses on activities and programs that recognize timely whether fraud or misconduct has occurred or is occurring. Can preventive measures assure that fraud will not be committed? No, but preventive controls are the first line of defense in minimizing fraud risk.

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

Fraud-prevention controls may occur at the entity level or at the specific process level. For example, an organization may establish authoritative approval levels across the enterprise to serve as an entity-level control. In addition, individuals working within a specific function may have limited IT access to serve 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.

Fraud Risks

One key to prevention is expanding an awareness of the types of fraud and misconduct that may occur within the organization. Awareness of fraud and misconduct schemes is developed through periodic assessment, training, and frequent communication. This awareness should enforce the notion that all of the mechanisms established in the antifraud program are real and will be enforced. The ongoing communication efforts could provide information on the potential jail sentence and/or fines and the resulting effects on the individual such as professional ruin, personal financial ruin, divorce, and potentially being labeled a felon.

The system of internal control 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 components, principles, and concepts for enterprise risk management for all organizations regardless of size.

However, internal controls may or may not address the organization's fraud risks. Fraud risks can differ from business risks and necessitate a higher level of control to mitigate. So the fraud risk assessment process is essential to the prevention program.

In addition to the issues surrounding the COSO components in Section 2 regarding corporate governance, the following subjects need to be continuously reviewed for improprieties:

- *Third-party Transactions* — Because fraud schemes often involve the use of third-party entities/individuals, organizations need thorough measures in 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.
- *Related-party Transactions* — Especially important are 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.
- *Financial Reporting Competencies* — Fraud is less likely when the organization employs highly competent individuals in financial reporting oversight roles. Experienced professionals who have undergone intensive interviews and background checks are more likely to be effective in preventing fraud because they have passed essential verification processes that attest to their integrity and have a more comprehensive understanding of fraud, its red flags, and its potential to devastate the organization.
- *Authority and Responsibility* — 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, especially misappropriation of assets.
- *Human Resources* — The sophistication of an organization's HR function can play an important role in fraud prevention by:

1. Performing Background Investigations. An organization is less likely to hire someone who has participated in illegal or inappropriate behavior in the past, or who displays behavioral tendencies that might suggest a heightened risk of such behavior in the future (e.g., lying or padding a résumé). Background checks also should be performed for existing employees who are candidates for promotion to officer status or to a position in which they will handle or have access to company assets. These checks can help ensure that even if the person has been employed for some time, nothing has occurred since they were hired that the company is not aware of — such as a bankruptcy or pending large monetary judgment against the individual — that may influence a decision to promote.

Likewise, examinations should be performed on critical suppliers and customers to verify their financial soundness and validity. The same should be done for key business partners with which the organization may enter into any type of business arrangement.

2. Hiring Competent Personnel and Antifraud Training. By hiring competent individuals, especially in financial reporting oversight roles, fraud is more likely to be prevented or detected. New hires may arrive at an employer with little or no exposure to antifraud programs. They may not have seen or been asked to comply with a code of conduct or ethics before. As a result, they are most likely unfamiliar with the purpose or need for such a program.

An organization's HR group is often responsible for providing training on the code of conduct or ethics. The effectiveness of this training increases the likelihood that fraud will be prevented. A sound training program should explain the purpose of the antifraud program, and educate employees about the program, what constitutes fraud, and what to do when fraud is suspected. Training becomes paramount in maintaining the culture of the organization.

3. 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 as well as work-related competence. By conducting compensation surveys and local market analysis, HR can determine whether senior management and employees are properly compensated. Managers whose compensation is based largely on bonuses and other rewards may be inclined to cut corners or deliberately fabricate financial results.

4. 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 fraud and misconduct that could indicate conditions conducive to fraud. HR should also review the content and information contained in resignation letters because they often contain information regarding possible existing fraud and misconduct within the organization.

Control Activities

Control activities designed to mitigate fraud are not always the same as the organization's internal control activities designed to identify errors. The system of internal control is a process

affected by the people in the organization to provide reasonable — not absolute — assurance that the activities of the organization are conducted in accordance with the established policies and procedures set forth by management. Everyone in the organization is responsible for internal control.

Antifraud control activities, on the other hand, are either preventive or detective. They represent the actions taken by executive management to mitigate the specific fraud risks identified in the risk assessment process and are therefore more specialized in both their design and application. Some risks can have both preventive and detective controls associated with them. In fact, some risks may have multiple controls of either or both types that mitigate their occurrence.

Clearly, the risk assessment process drives the preventive control activities. Prevention is the most proactive fraud-fighting measure. The design and implementation of the control activities should be a coordinated effort spearheaded by management and the audit committee, with an assembled cast of employees, IT, and internal audit personnel. 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 that are used are adequate to prevent fraud from occurring.

The ongoing success of any 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 deterring and preventing fraud.

One of the more effective preventive measures organizations can implement is a whistleblower hotline¹³, which has markedly increased among SEC registrants since it was mandated by the Sarbanes-Oxley Act. Knowledge that an employee hotline is in place can help prevent fraud since fear that a fraud may be discovered and reported can deter a potential fraud 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.

A hotline should allow the caller to remain anonymous, thereby minimizing fears of reprisal from reporting such activities. This is one of the keys to a successful hotline. Another key is assurance that the notification will result in some action being taken. Marketing its existence to increase awareness, ease of use, and promoting the timely handling of all reported issues all represent strong preventive measures. 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. In addition, the board should deal swiftly with any attempts to bring harm to whistleblowers. A culture of over-reporting and effective and swift handling should be encouraged.

¹³ Whistleblower hotlines are a U.S.-centric policy and may not be legal or ethical in countries outside the United States. Countries such as France have indicated that these activities may violate privacy laws. As such, multinational organizations may not be able to implement hotlines on a worldwide basis.

It is essential that any violations, deviations, or other breaches of the code of conduct be dealt with in a timely manner and appropriate punishment imposed, and for suitable remediation to be completed. The board should ensure this includes the members of top management as well. As delegated by the board, the audit committee should provide for the proper dissemination of information concerning breaches of antifraud policies throughout the organization as an indication of the diligence of the program and its success in preventing fraud.

The organization's plan, approach, and scope of monitoring the fraud-prevention program should be documented and updated as required. 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 the program be monitored by an independent entity. But the reviews should be conducted separately from any routine or planned audits and be designed to assure management of the effectiveness of the program.

Before each review, issues such as significant changes in the organization and its 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 antifraud 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 5: FRAUD DETECTION

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

One of the strongest deterrents to fraud is the perception that effective detective controls are in place. Combined with preventive controls, detective controls enhance the effectiveness of an antifraud program by providing evidence that preventive controls are working as intended and identifying fraud if it occurs. Although detective controls may provide evidence that fraud has occurred, or is occurring, 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 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 detective controls may be necessary based on the fraud risks identified for the organization.

Detective Controls

Every organization is susceptible to fraud, but not all fraud can be prevented, nor is it cost-effective to try. As approved by the board, an organization may choose to design its controls to detect rather than prevent certain fraud schemes. However, if the estimated cost of the controls — such as tools, personnel, or training — exceeds the estimated impact of the scheme, 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. Three important detection methods are: an anonymous reporting mechanism (i.e., hotline), internal auditing, and process-related controls specifically designed to detect fraudulent activity.

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, 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 controls needed to reduce and control the risks. Each industry is susceptible to different types of fraud schemes. The process becomes more cumbersome in organizations that span different industries. Organizations with multiple divisions/business units will find it necessary to first perform a broad organization wide assessment and then perform more detailed and focused assessments of individual business units.

Anonymous Reporting

Various surveys¹⁴ indicate that anonymous tips are the most likely means of detecting fraud. Provision for anonymity should be guaranteed to any individual who openly and willingly comes forward to report a suspicion of fraud. Employees should also be assured that they will not be retaliated against for reporting their suspicions of wrongdoing by their superiors.

A hotline should provide anonymity to the caller to be effective. The most effective hotlines proactively demonstrate confidentiality to potential callers through techniques such as the use of an independent hotline operator. Hotlines ideally support a multilingual capability and provide access to a trained interviewer 24 hours a day, 365 days a year. 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 as the board's designee.

The importance of gaining the confidence of an organization's vendors, suppliers, and customers cannot be underestimated. Industry-specific sources relay information, both good and bad, about their customers and vendors that can be an invaluable source of information that cannot be gathered within an organization. Hotlines have proven to be extremely successful in this regard.

¹⁴ The ACFE Occupational Fraud and Abuse Survey and the KPMG Fraud Survey are examples.

The board should approve protocols to ensure 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/functional area has this highly sensitive information and increases accountability.

Finally, 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 antifraud program to address evolving risks. The hotline program should be independently evaluated periodically for effectiveness, including compliance with established protocols.

Internal Auditing

Although management and those charged with governance are responsible for assessing fraud risks and designing internal controls to prevent, detect, and mitigate those fraud risks, internal auditors are an appropriate resource for assessing the effectiveness of what management has implemented. The importance an organization attaches to its internal audit function is an indication of the organization's commitment to effective internal control. An internal audit department's charter or mission statement — which should be approved by the audit committee — should direct the role of internal auditing in an antifraud program.

Internal auditors should consider the organization's assessment of fraud risk when developing their annual audit plan and periodically assess management's fraud-detection capabilities. They should also interview and regularly communicate with those conducting the assessments, as well as others in key positions throughout the organization, to help them assess whether all fraud risks have been considered. When performing engagements, internal auditors should devote sufficient time and attention to evaluating the design and operation of internal controls related to preventing and detecting significant fraud risks. They should exercise professional skepticism when reviewing activities to be on guard for the signs of potential fraud. Potential frauds uncovered during an engagement should be treated in accordance with a well-defined response plan consistent with professional and legal standards.

Effective internal audit departments are adequately funded, staffed, and trained, with appropriate specialized skills given the nature, size, and complexity of the organization and its operating environment. Internal auditors should be aware of and trained in the tools and techniques of fraud detection, response, and investigation as part of their continuing education program. The department should be independent (authority and reporting relationships), have adequate access to the audit committee, and adhere to professional standards.

Proactive Fraud Detection

In addition to detective process controls, organizations may be able to effectively use data analysis and continuous auditing techniques 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. Data analysis allows users to identify relationships between people, organizations, and events.

Proactive consideration of how certain fraud schemes may result in identifiable types of transactions or trends enhance an organization's ability to design and implement effective data analysis. Data analytics can also be used to cost-effectively ensure that other fraud-prevention and detection controls in place are effective.

Continuous auditing is the use of data analytics on a continuous or real-time basis, thereby allowing management or internal auditing to identify and report fraudulent activity more rapidly. For example, a Benford's Law analysis¹⁵ can be used to 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.

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 will need to periodically assess the effectiveness of process controls, anonymous reporting, and internal auditing.

Characteristics of Fraud Detection

Fraud can never be eliminated from businesses and other organizations entirely. There will always be an opportunity for someone in any organization to override a control or collude with others to do so. Therefore, detective mechanisms 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 that 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.

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

- Identify hidden relationships between people, organizations, and events.
- Identify suspicious transactions.
- Assess the effectiveness of internal controls.
- Monitor fraud threats and vulnerabilities.

¹⁵ Benford's Law analysis is a process of comparison of actual results vs. expected results by looking for unusual transactions that do not fit an expected pattern.

- Consider and analyze thousands or millions of transactions.

Evidence of fraud can sometimes be found in e-mail. 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 entity's risk analysis.

Some internal audit departments or consulting firms, as part of their fraud-detection efforts, have developed tools that analyze journal entries for examination 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 ID, date of entry, and unusual account pairings.

Organizational Roles

A robust and effective fraud-detection program starts with those charged with establishing and maintaining an effective governance program. This body establishes the program and provides the resources to ensure its success. Although a fraud-detection program and the parameters of that program are overseen by the board or the audit committee, it is the responsibility of all managers to manage the risks of fraud and misconduct in their organization. Management should communicate throughout the organization all actions taken against fraudsters to reinforce the commitment to ethical standards and integrity.

Documentation of Detection Program and Techniques

An organization should formally document the techniques and components developed and instituted to detect frauds that breach the internal control system. This includes documenting processes used to monitor the performance of other antifraud controls or to indicate when other antifraud controls are ineffective. Testing procedures conducted to ensure adequate operation of fraud-detection controls and the testing results should also be thoroughly documented.

Paramount to this documentation is a detailed description of the elements of the organization's fraud-detection program, with emphasis placed on the roles and responsibilities of all parties involved in the fraud-detection process. 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 plan 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 development phase of the plan, 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 related to fraud-detection controls.

Once the final 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 deterrence measure. By communicating this to employees, vendors, shareholders, and others, the organization affirms that it has a detection plan in place and that it takes fraud seriously without revealing all the relevant characteristics of the plan.

Measurement Techniques

The organization should develop ongoing monitoring and measurement techniques to evaluate, remedy, and continuously improve the organization's fraud-detection program. If deficiencies are detected, 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 board or chief ethics officer of the organization should establish measurement criteria to monitor and improve compliance with fraud-detection controls. These measures should be provided to the board.

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 including controls in place, fraud risks identified, and resources available. Examples of specific measurement techniques are:

- Reporting on the lack of recurrence of frauds uncovered.
- Reporting on the timeliness of implementation of remediation plans.
- Promptly adding additional controls to prevent new frauds.
- Addressing the likelihood that frauds perpetrated against other organizations in the same industry will occur in the organization.
- Reporting of fraud versus complaints, grievances, etc., via hotline calls.
- Reporting of the number of frauds discovered versus the number of fraud audits performed.
- Reporting 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 6: INVESTIGATION AND RESPONSE

Principle 5: A reporting process should be in place to solicit inputs on potential fraud events and a coordinated investigation approach should be used to ensure potential fraud events are dealt with in a timely manner.

Receiving the Allegation

A case of potential fraud may arise in many different ways: 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 clearly defined 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(s).

- Defining the severity of the allegation(s).
- 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.

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 an individual or individuals designated to conduct an initial evaluation of the allegation. This person or persons should have the necessary authority and skills to evaluate the allegation and determine the appropriate course of action to resolve it. In cases that involve the board or top 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 should also be advised of any fraud that could affect the organization's financial statements.

Instituting a Case Management System

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.

Cases Involving Senior Management Misconduct or Financial Statement Manipulation

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, then 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 should include:

- *Time-sensitivity* — Could be 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* — Keeping the information confidential and ensuring distribution is 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* — Compliance with applicable laws and rules regarding gathering of information and interviewing witnesses.
- *Securing evidence* — Protecting evidence so that it is not destroyed and so that it is admissible in legal proceedings.
- *Objective* — The investigation team should be sufficiently removed from the issues and individuals under investigation to conduct an objective assessment.
- *Goals* — Specific issues or concerns that should appropriately influence the focus, scope, and timing of the investigation.

Responsibility for overseeing an investigation should be given to a party 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. The following should be considered to determine if their participation is necessary:

- Legal counsel.
- Internal and external auditors.
- Accountants/forensic accountants.
- HR personnel.
- Security/loss prevention personnel.
- IT personnel.
- Computer forensics experts.
- Management representative.

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. An investigation team leader should be chosen to coordinate the investigation and interface with management as necessary. The roles and responsibilities of each team member should be clearly communicated. 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.

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.

Investigations generally include many of the following tasks:

- Interviewing, including:
 - Neutral third-party witnesses.
 - Corroborative witnesses.
 - Possible co-conspirators.
 - The accused.
- Evidence collection, including:
 - Internal documents, such as
 - Personnel files.
 - Internal phone records.
 - Computer files.
 - E-mail.
 - Financial records.
 - External records, such as
 - Public records.
 - Customer/vendor information.
 - Media reports.
 - Information held by third-parties.
- Evidence analysis, including:
 - Review and categorization of information collected.
 - Computer-assisted data analysis.
 - Development and testing of hypotheses.
- Computer forensic examinations.

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.

Recovery/Corrective Actions

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

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. The organization's chief legal counsel should make the decision as to whether criminal prosecution is appropriate.
- *Civil action* — The organization may wish to pursue its own civil action against the perpetrator(s) 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 investigations* — 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, employees, shareholders, investors, 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 three may be relatively simple and powerful:

- *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 including an estimate of future losses prevented can help to demonstrate the value of antifraud actions.

SECTION 7: CONCLUDING COMMENTS

Planning for the proper reaction to potential fraud risks and monitoring responses taken are the cornerstone actions that organizations can take to mitigate exposure to fraudulent activities. Although complete elimination of any fraud risk is most likely uneconomical, organizations can take positive and constructive steps to identify and consider the appropriate actions that can prevent and/or detect undesired actions. Most organizations use control techniques that serve both to ensure the accuracy of information and to help mitigate fraud risks. It is important that when these dual roles for controls exist, the outputs of these control techniques are provided to the right people to ensure review for both control objectives.

The real focus of managing fraud risks should be to discourage fraud, prevent employees from having the opportunity to perpetrate a fraud against the organization, and to protect the organization from employees who intend to commit fraud. A sound approach is to understand fraud risks within the organization from the board on down, have an actively engaged board, set the right board and management tone regarding fraud risk tolerance, ensure appropriate responses to potential fraud risks have been put in place, and monitor results to ensure those responses are effective. The ideas in this paper will help any organization taking up this challenge to address this key business concern in an organized, meaningful, and balanced manner.

APPENDIX A: REFERENCE MATERIAL

For Executives

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

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

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

Association of Certified Fraud Examiners (ACFE)/AICPA, *Tone at the Top: How Management Can Prevent Fraud in the Workplace*, 2006, www.acfe.com/fraud/tools.asp [white paper and video].

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

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 20, 2007), www.sec.gov/rules/interp/2007/33-8810fr.pdf.

Fraud Risks

ACFE, *2006 ACFE Report to the Nation on Occupational Fraud & Abuse*, 2006, www.acfe.com/documents/2006-rtn.pdf.

Ernst & Young LLP, "9th Global Fraud Survey—Fraud Risk in Emerging Markets," 2006, [http://www.ey.com/global/assets.nsf/International/FIDS_-_9th_Global_Fraud_Survey_2006/\\$file/EY_Fraud_Survey_June2006.pdf](http://www.ey.com/global/assets.nsf/International/FIDS_-_9th_Global_Fraud_Survey_2006/$file/EY_Fraud_Survey_June2006.pdf)

Transparency International, "TI Corruption Perceptions Index," 2007, www.transparency.org/policy_research/surveys_indices/cpi.

U.S. Department of Justice, "Principles of Federal Prosecution of Business Organizations," 2006, www.usdoj.gov/dag/speeches/2006/mcnulty_memo.pdf.

Fraud Controls

U.S. Sentencing Commission, *2005 Federal Sentencing Guidelines Manual*, Chapter Eight: Sentencing of Organizations, 2005, www.usssc.gov/orgguide.htm.

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

KPMG LLP, *Fraud Risk Management: Developing a Strategy for Prevention, Detection, and Response*, 2006, www.us.kpmg.com/services/content.asp?11id=10&12id=30&cid=2290.

PricewaterhouseCoopers LLP, *Key Elements of Antifraud Programs & Controls*, 2003, www.pwc.com/images/gx/eng/fs/insu/rt6.pdf.

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

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

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

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

The Network, *Best Practices in Ethics Hotlines*, 2004, www.tnwinc.com/news/downloads/TNW-RLHOTWP2-CM.pdf.

The Network, CSO Executive Council, and ACFE, *2006 Corporate Governance and Compliance Hotline Benchmarking Report*, 2006, www.deloitte.com/dtt/article/0,1002,sid=2007%26cid=151001,00.html.

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

Internal Auditing

The Institute of Internal Auditors (IIA), *Practice Advisory 1210.A2-2: Auditor's Responsibilities Relating to Fraud Investigation, Reporting, Resolution, and Communication*.

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

General

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

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

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

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

ACFE, *2006 Fraud Examiners Manual*, 2006.

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

The Chartered Institute of Management Accountants, *Fraud Risk Management—A Guide to Good Practice*, 2001.

HM Treasury, Assurance, Control, and Risk, *Managing the Risk of Fraud: A Guide for Managers*, 2003.

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

APPENDIX B1: FRAUD GOVERNANCE POLICY CONTENT

Suggested Framework for Fraud Control Policy (Or Plan)¹⁶

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

¹⁶ Reference: The Australian Standard on Fraud and Corruption Control, AS 8001-2003.

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 B2: SAMPLE FRAUD POLICY¹⁷

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.

¹⁷ Reference: 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 clearly explain 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 be 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

Fraud Policy Decision Matrix

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 C1: FRAUD RISK ASSESSMENT FRAMEWORK EXAMPLE

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.

Fraud Risks Identified (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Antifraud Controls (5)	Assess Effectiveness of Controls (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		Periodic testing by IA
• Channel stuffing	Remote	Insignificant	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.	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 .	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

Fraud Risks Identified (1)	Likelihood (2)	Significance (3)	People and/or Department (4)	Antifraud Controls (5)	Assess Effectiveness of Controls (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. **Fraud Risks Identified:** This column should include a full list of the potential fraud and misconduct risks that may face the organization. This list of risks 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 of the Fraud Risk:** To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks such that the organization establishes proper antifraud 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 or 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. **Antifraud Internal Controls:** Map pre-existing controls to the relevant fraud risks identified. Note, this occurs subsequent to fraud risks being identified and being 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:** 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 Sarbanes-Oxley 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, certain fraud risks may not be adequately mitigated 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 the 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 C2: FRAUD RISK EXPOSURES¹⁸

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 C1 could be used¹⁹.

- 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 & 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

¹⁸ The Fraud Risk Manual issued by the ACFE, 2007.

¹⁹ 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 D: FRAUD PREVENTION SCORECARD

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

-  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 <i>Code of Organizational Conduct</i> 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 <i>Enterprise Risk Management–Integrated Framework</i> and have taken specific actions to strengthen our prevention mechanisms as necessary.		
We have adequately assessed fraud risk for our organization 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 adequately addressed the strengths and weaknesses of our internal control environment and have taken specific steps to strengthen the internal control structure to help prevent the occurrences of fraud.		

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 carefully assessed all overseas and decentralized operations and have taken proactive steps to assure that they have fraud-prevention 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 assure 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-prevention 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.		
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 <i>any</i> 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 <i>Code of Organizational Conduct</i> .		
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 <i>Code of Organizational Conduct</i> . All concerns resulting from these interviews are communicated to our audit committee.		
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-prevention mechanisms on an ongoing basis and document these reviews as well as the communication of needed areas for improvement to the audit committee.		

<p>We have a fraud response plan in place and know how to respond if a fraud allegation is made. The fraud response plan considers:</p> <ul style="list-style-type: none">• 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 E: FRAUD DETECTION SCORECARD

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



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-detection 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.		

We take steps to assure 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.		
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 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 between 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.		
<p>Our fraud-detection documentation identifies the individuals and departments responsible for:</p> <ul style="list-style-type: none"> • 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. 		

<ul style="list-style-type: none"> • 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. 		
<p>We have established measurement criteria to monitor and improve compliance with fraud-detection controls, including:</p> <ul style="list-style-type: none"> • 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 requirements. • Number of customers who have signed the organization’s ethical behavior requirements. • Number of fraud audits performed by internal auditors. 		
<p>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.</p>		

APPENDIX F: ALIGNMENT OF PRINCIPLES TO OCEG FOUNDATION

Below is a summary listing of the practices in the OCEG Foundation²⁰ 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.

²⁰ © 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, and
- forensic investigations.

APPENDIX G: COSO FRAUD RISK MANAGEMENT ACTIVITIES PER THE 1992 FRAMEWORK

<p>Control Environment</p>	<p>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.</p>
<p>Fraud Risk Assessment</p>	<p>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.</p>
<p>Antifraud Control Activities</p>	<p>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.</p>
<p>Information and Communication</p>	<p>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.</p>
<p>Monitor</p>	<p>Providing periodic evaluation of antifraud 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.</p>