Key Elements of Antifraud Programs and Controls

A White Paper

This white paper provides general or summary information about aspects of the Sarbanes-Oxley Act of 2002 and current and proposed rules, regulations and standards of the U.S. Securities and Exchange Commission, Public Company Accounting Oversight Board and national securities exchanges and associations. The information and considerations presented do not constitute the provision of legal advice. Boards of directors, audit committees and companies are encouraged to refer to the foregoing statute, rules, regulations and standards, and to consult with legal counsel concerning their responsibilities with respect to applicable provisions thereof.

Table of Contents

The general or summary information provided in this paper was developed as of November 2003. PricewaterhouseCoopers accepts no responsibility for reporting changes in the law and current and proposed rules, regulations or standards referred to herein or their interpretation, which may occur after that date. The information contained herein is provided for use by U.S. issuers whose securities are listed on national securities exchanges or associations. While aspects of this paper may apply, or be of interest, to non-U.S. issuers or other specialized entities, the information was not developed to meet their specific needs.

I. Background

Political & Legislative Context

In 2002, Congress passed the Sarbanes-Oxley Act[1], designed to restore shareholder confidence in publicly traded securities following a series of highly publicized corporate scandals. Subsequently, the Securities and Exchange Commission, New York Stock Exchange, National Association of Securities Dealers[2] and Public Company Accounting Oversight Board[3] adopted and proposed rules and regulations mandating programs and processes tailored to meet the requirements of the new law.[4] Allowing for relatively minor variations in applicability and specifics, the new regulations all have the same goals:

- Provide greater transparency in corporate accounting and reporting
- Provide greater accountability by making board members and executives personally responsible for financial statements
- Place greater emphasis and structure around efforts to prevent, detect, investigate and remediate fraud and misconduct

Responsibility for managing the company and preparing financial statements has traditionally rested with management and the board of directors. The new law makes it abundantly clear, if there was ever any doubt, that these individuals are also responsible for establishing, validating and monitoring effective internal controls to prevent fraudulent financial reporting — and to detect it on a timely basis when it does occur.

So, What Is Fraud?

Fraud is a broad concept that refers generally to any intentional act committed to secure an unfair or unlawful gain.[5] Financial fraud typically falls into four broad categories:

- **Fraudulent financial reporting** — Most fraudulent financial reporting schemes involve earnings management, arising from improper revenue recognition, and overstatement of assets or understatement of liabilities.

---

1 Sarbanes-Oxley Act of 2002, 15 U.S.C. §7201 (2002).
2 On Nov 4, 2003, the SEC approved the New York Stock Exchange, Inc. ("NYSE" or "Exchange") proposed rule change (SR-NYSE-2002-33, August 16, 2002), as amended by NYSE Amendment No. 1 (April 4, 2003) and the Nasdaq Independent Director Proposal (SR-NASD-2002-141, October 9, 2002), as amended; the Nasdaq Going Concern Proposal (changes SR-NASD-2002-77); the Nasdaq Related Party Transactions Proposal (SR-NASD-2002-80), as amended; the Nasdaq Issuer Applicability Proposal (SR-NASD-2002-138), as amended; and the Nasdaq Code of Conduct Proposal (SR-NASD-2002-139).
3 Proposed Auditing Standard – *An Audit of Internal Control Over Financial Reporting Performed In Conjunction With An Audit of Financial Statements,* Public Company Accounting Oversight Board Release No. 2003-017 (October 7, 2003) [hereinafter "PCAOB"].
4 See Appendix A for highlights of antifraud laws, regulations and standards.
5 Black's Law Dictionary defines fraud as, "An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right; a false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury."

- **Misappropriation of assets** — This category involves external and internal schemes, such as embezzlement, payroll fraud and theft.

- **Expenditures and liabilities for improper purposes** — This category refers to commercial and public bribery, as well as other improper payment schemes.

- **Fraudulently obtained revenue and assets, and costs and expenses avoided** — This category refers to schemes where an entity commits a fraud against its employees or third parties, or when an entity improperly avoids an expense, such as tax fraud.

Antifraud Mantra: Prevention and Timely Detection

Companies subject to Sarbanes-Oxley must now implement “antifraud programs and controls” that are evaluated annually during the integrated audit[6]. Although most of these companies have already implemented components of an antifraud program such as codes of ethics and conduct, they may need to enhance their programs to meet the requirements of the new law and to avoid an auditor’s finding of a “significant deficiency” or “material weakness” in internal controls[7]. Private companies should also have an understanding of effective fraud management, particularly if their strategy contemplates a public debt offering, IPO or sale to a public company. Apart from mitigating legal and regulatory risk, fraud management provides significant cost savings[8] opportunities, which directly affect the bottom line.

Although Congress, the SEC and PCAOB have not yet delineated what constitutes an effective antifraud program and controls, PricewaterhouseCoopers has identified the key elements of an effective antifraud program based on the core principles shared by the new law, regulations and standards: prevention and timely detection of fraud.

The COSO Framework

Management must base its assessment of the effectiveness of the company’s internal control over financial reporting on a suitable, recognized control framework established by a body of experts. In the United States, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission has published the *Internal Control – Integrated Framework* (known as the “COSO Report”), which has emerged as the framework that management and auditors use to evaluate internal controls. Accordingly, we apply the COSO framework[9] because most companies and auditors in the United States use COSO to assert and audit the effectiveness of internal controls.

---

6 PCAOB at ¶24.
7 See Appendix B for definitions of significant deficiency and material weakness.
8 The Association of Certified Fraud Examiners (ACFE) projects that (1) the average company loses the equivalent of six percent of its revenue to fraud and (2) fraud annually accounts for $600 billion in losses. ACFE, *2002 Report to the Nation, Occupational Fraud and Abuse.*
9 Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control – Integrated Framework* [hereinafter “COSO”].

Applying the five elements of COSO (control environment, risk assessment, control activities, information and communications, and ongoing monitoring), this white paper (1) enumerates the attributes of good program design and operating effectiveness and (2) provides guidance regarding the kinds of deficiencies that typically result when one or more of these key elements is absent or ineffective.

Although antifraud programs and controls must include all five components of COSO, special emphasis is on the control environment, the tone set at the top of an organization that influences the control consciousness of its people.

II. Applying the Five COSO Elements

Control Environment

The control environment refers to such intangibles as integrity, ethical values and competence of the entity's people, and management's philosophy and operating style, but it also covers more concrete expressions of these intangibles, such as the way management assigns authority and responsibility, and organizes and develops its people. In addition, the control environment sets out the role of the audit committee and board of directors. The control environment has a pervasive influence on the way business activities are structured, objectives are established and risks assessed. It also influences risk assessment, control activities, information and communication systems, and monitoring activities. The control environment is not static; it is influenced by the entity's history and culture and in turn influences the "control consciousness" of its people in performing their day-to-day activities. Since 90% of the frauds occur in the C-Suite[1], the establishment of strong antifraud programs and controls is an essential component of a healthy control environment.

Code of Conduct/Ethics

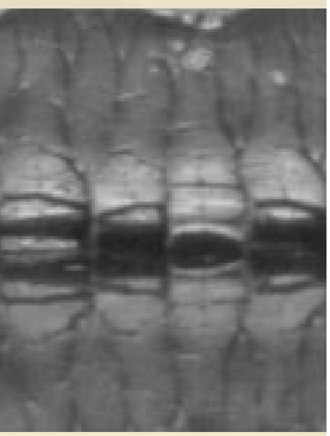
Sarbanes-Oxley §406 and the SEC's Final Rule entitled "Disclosure Required by Sections 406 and 407 of the Sarbanes-Oxley Act of 2002" require a registrant to disclose whether it has adopted a code of ethics that applies to the company's principal executive officer, principal financial officer, principal accounting officer or controller, or persons performing similar functions. If it has not adopted such a code of ethics, it must explain why. The NYSE and NASDAQ rules require the adoption and public disclosure of a code of business conduct and ethics that applies to all directors, officers and employees and outlines specific topics that must be addressed.

The term "code of ethics" is defined in the Final Rule as written standards that are reasonably designed to deter wrongdoing and to promote:

- Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships

---

1 "Defrauding the Public Interest: A Critical Examination of Reengineered Audit Processes and the Likelihood of Detecting Fraud," Charles P. Cullinan and Steve G. Sutton.



- Full, fair, accurate, timely and understandable disclosure in reports and documents that a registrant files with, or submits to, the SEC and in other public communications made by the registrant
- Compliance with applicable governmental laws, rules and regulations
- The prompt internal reporting of violations of the code to an appropriate person or persons identified in the code
- Description of what constitutes fraudulent behavior
- Accountability for adherence to the code and the sanctions to be imposed on those who breach it

Design and Documentation

An effective code of conduct is a fundamental element of an effective control environment and antifraud program. A company's code of conduct should apply to all persons in an accounting or financial reporting oversight role, which includes all persons who are (1) in a position to, or do, exercise influence over the contents of the financial statements or (2) over anyone who prepares them through, for example, direct responsibility or oversight of those persons, such as when the person is a member of the board of directors or similar management or governing body, chief executive officer, president, chief financial officer, chief operating officer, general counsel, chief accounting officer, controller, director of internal audit, director of financial reporting, treasurer, director of tax or any equivalent position.

Due to the potential for apparent or actual conflicts of interest, the code of conduct should apply internally and externally, that is, to anyone who has significant influence over relationships and dealings with suppliers, customers, investors, creditors, insurers, competitors, auditors and so forth. It should articulate what constitutes fraudulent behavior, how accountability for the code is established and the sanctions imposed for noncompliance. It should address conflicts of interest; corporate opportunities; confidentiality of information; fair dealing; protection and proper use of company assets; related party transactions; illegal acts; compliance with laws, rules and regulations; and the monitoring of the code by management. *Any waivers of the code for directors or executive officers should be approved by the board and disclosed promptly in an 8-K by registrants.* The code should outline clear and objective standards for compliance and set up a fair process to determine violations. The board of directors and audit committee have key oversight roles with respect to the code of conduct. Evidence of their oversight role should be documented in the board of directors and audit committee charters and meeting minutes.

Furthermore, as a best practice, we believe a code of conduct should include all employees to ensure that any observed instances of misconduct or pressure to compromise ethics standards are reported.

Operating Effectiveness

The mere existence of a code of conduct does not evidence its effectiveness.

- The code of conduct also must be communicated effectively (through the employee handbook, policy manual, intranet, etc.) on a periodic basis to all covered persons. Ineffective communication prevents even a comprehensive code of conduct from being effective and contributing to an appropriate "tone at the top."

- Employees should evidence their receipt and reading of the code. This is generally accomplished through a confirmation process. Annual confirmations from the covered persons regarding their compliance (or lack thereof) with the code of conduct, including appropriate follow-up regarding lack of response and any exceptions noted, provide adequate evidence.

- Requiring attendance at training at the time of hiring and periodically thereafter evidences the entity's commitment to ensuring that the employees understand the code. Training should address the "tone at the top," code of conduct, and the individual's duty to communicate or report actual or suspected fraud or misconduct. Interactive training may provide evidence that a code has been communicated, and that employees have received, read and understood the code.

- Both management and the audit committee are required to monitor the code of ethics. Meeting minutes should evidence their ongoing or periodic monitoring.

Chapter 8 of the U.S. Sentencing Guidelines Manual states that an "effective program to prevent and detect violations of law" means a program that has been reasonably **designed**, **implemented** and **enforced** so that it generally will be effective in preventing and detecting criminal conduct. Accordingly, a company must undertake reasonable measures to be sure that employees understand the concepts embodied in the code of conduct.

Evaluation of Deficiencies

A company's failure to have a documented code of conduct approved by the board of directors and its audit committee that is operating effectively is, at a minimum, a significant deficiency and a strong indicator of a material weakness. The code of conduct should address both internal and external dealings and cover, at a minimum, all individuals in an accounting or financial reporting oversight role.

Operating effectiveness is evidenced by:
- Plan to communicate the code to the covered people
- Annual confirmation process
- Training upon hiring and periodically thereafter
- Audit committee involvement and oversight

The PCAOB Proposed Auditing Standard indicates that "controls related to the prevention, identification, and detection of fraud in the control environment often have a pervasive effect on the risk of fraud."[2] The paragraph specifically sets forth specific provisions the code should include as well as how management and the audit committee or board of directors should monitor the code. Consequently, the omission of audit committee involvement and oversight is a strong indicator of a significant deficiency related to internal control over financial reporting. Furthermore, effective implementation and enforcement of the Code of Ethics/Conduct should be evidenced through some form of ongoing communication such as confirmation or training.

Ethics Hotline/Whistleblower Program

Sarbanes-Oxley §301, the SEC's Final Rule entitled "Standards Relating to Listed Company Audit Committees," and the listing standards called for by this Final Rule require each issuer's audit committee to establish procedures for:

- Receiving and retaining information about, and treating alleged incidents involving the issuer regarding accounting, internal accounting controls or auditing matters
- The confidential, anonymous submission of concerns by employees about questionable accounting or auditing matters

Design and Documentation

The Final Rule does not mandate specific procedures the audit committee must establish, as the SEC believes audit committees should have the flexibility to develop and use procedures appropriate for their circumstances.

All public companies subject to Sarbanes-Oxley §404 – not just listed companies – should have an ethics hotline or whistleblower program similar to that required by Sarbanes-Oxley §301. The ethics hotline should provide employees and others a means of:

- Communicating concerns, anonymously if preferred, about potential violations of the code of conduct, including unethical behavior and actual or suspected fraud, without fear of retribution
- Obtaining advice before making decisions that appear to have significant legal or ethical implications

This program should operate independently of management. This independence can be achieved through administration of the program by an independent third party to provide the intake mechanism, or by establishing a neutral party within the organization, such as an ethics or compliance officer or internal auditor with appropriate experience and objectivity, who reports directly to the audit committee. An appropriate communication mechanism for reporting potentially troublesome matters to the audit committee and external auditor also should be in place. The audit committee should provide independent review and follow-up.

---

2 Proposed Auditing Standard – *An Audit of Internal Control Over Financial Reporting Performed In Conjunction With An Audit of Financial Statements,* ¶24, Public Company Accounting Oversight Board Release No. 2003-017 (October 7, 2003).

It is the audit committee's responsibility to oversee the procedures established by management for this program and ensure that any reported matters are communicated to the audit committee and/or board. The audit committee has a responsibility to review periodic reports on the nature, status and disposition of alleged or suspected fraud to be confident that they have been notified about all matters that should have been reported and that appropriate communications have taken place.

Adequate documentation of the process should exist. In addition, internal audit or an independent party should conduct a walk-through of the hotline/whistleblower process to assist the audit committee in understanding the process. The walk-through should trace the different types of calls received, from initial receipt of information through the company's process for follow-up and resolution to notification of the audit committee where appropriate. Feedback solicited from callers also can provide insight into the appropriateness of the design.

Operating Effectiveness

The operating effectiveness of the hotline or whistleblower program should be assessed. Considerations include: Are employees aware of the hotline? Is reporting of alleged incidents encouraged? Are people actually reporting possible instances of misconduct? Is follow-up appropriate and timely? Do employees use the hotline to get advice for difficult decisions? The process should be tested through an examination of the various communications and a sample of alleged incidents. Because a hotline is essentially a passive process that relies on the initiative of individual employees, volume of use may be a good indicator of effectiveness, providing insight into whether people believe they are encouraged to report an alleged incident. A pulse survey or "walkabout" (corroborating through inquiries of employees and by making calls to customers and vendors) may also provide insight into employees' views and their willingness to use the hotline. Evidence of active audit committee involvement should be obtained through discussions with audit committee members and internal or external counsel. Involvement should also be reflected in the audit committee minutes and in reports noting violations and subsequent actions.

Evaluation of Deficiencies

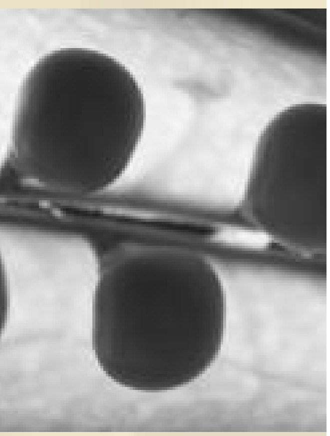
An effective ethics hotline/whistleblower program is both a fraud deterrent and an important means of discovering actual and suspected fraud. Absence of such a program constitutes potential non-compliance with Sarbanes-Oxley, as well as with the SEC's Final Rule and the listing standards. For these reasons, lack of an adequately designed and effective ethics hotline or whistleblower program is a strong indicator of a significant deficiency in internal control over financial reporting.

Hiring and Promotion

Establishing standards for hiring and promoting the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior, demonstrate an entity's commitment to competent and trustworthy people[3]. Such standards should include the performance of background investigations on individuals being considered for employment or for promotion to certain positions of trust within an organization. If some or all of these investigations were performed when an individual was hired, they need not be duplicated at promotion. Such positions include all persons in an accounting or financial reporting oversight role as defined earlier as well as other individuals, such as security officers, who have direct access to company assets or information systems.

Design and Documentation

The scope of the background investigation should cover all of the following areas:



- Educational background
- Employment history
- Criminal record

This process should be documented. In addition, PricewaterhouseCoopers recommends interviews with independent references as a best practice for organizations. Internal audit or an independent party working on behalf of the audit committee should conduct a walk-through of the background investigation process.

Operating Effectiveness

Human resources should have background investigations performed and keep a record in the employee files. The effectiveness of the investigation program should be tested by checking a sample of individuals to determine whether investigations are being performed and whether appropriate documentation is being maintained.

Evaluation of Deficiencies

An entity's failure to perform substantive background investigations, touching on all of the areas identified, for individuals being considered for employment or for promotion to those positions outlined above would be a strong indicator of a significant deficiency in internal control over financial reporting. The federal sentencing guidelines support this.

---

3 A company should also conduct appropriate integrity diligence prior to entering joint ventures, mergers and acquisitions or relationships with strategic suppliers, vendors and consultants.

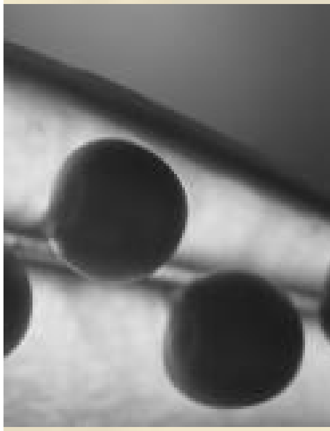
Oversight by the Audit Committee and Board

The board in its fiduciary role is responsible for overseeing the internal controls over financial reporting established by management and the process by which management satisfies itself that they are working effectively. The board is also responsible for assessing the risk of financial fraud by management and ensuring controls are in place to prevent, deter and detect fraud by management. Much of the audit committee's oversight is embedded in the other elements of an effective antifraud program.

The organization's board of directors and audit committee significantly influence the control environment and "tone at the top." The audit committee should be free from management's influence.

Design and Documentation

It is critical that the audit committee and the board of directors systematically and periodically review the internal controls over financial reporting established by management and that such responsibilities for oversight are reflected in their charters. Oversight should extend to:



- Management's antifraud programs and controls, including management's identification of fraud risks and implementation of antifraud measures
- The potential for management override of controls or other inappropriate influence over the financial reporting process
- Mechanisms for employees to report concerns
- Receipt and review of periodic reports describing the nature, status and eventual disposition of alleged or suspected fraud and misconduct
- An internal audit plan that addresses fraud risk and a mechanism to ensure that the internal audit can express any concerns about management's commitment to appropriate internal controls or to report suspicions or allegations of fraud
- Involvement of other experts – legal, accounting and other professional advisers as needed to investigate any alleged or suspected wrongdoing brought to its attention
- Review of accounting principles, policies and estimates used by management in determining significant estimates
- Review of significant non-routine transactions entered into by management
- Functional reporting by internal and external auditors to the board and audit committee

Operating Effectiveness

Appropriateness of oversight of the board and audit committee as it relates to fraud should be evidenced through discussions with board and audit committee members or reported in the committee meeting minutes. The board and the audit committee act independently from management. The scope of their oversight should include:

- Consideration of the nature and frequency of meetings of the board and audit committee and assessment of whether adequate meeting time is dedicated to the consideration of fraud

- Ensuring that audit committee members consider fraud in their review of
  - Accounting principles, policies and estimates used by management
  - Significant non-routine transactions entered into by management
- Evaluation of management's assessment of fraud risk
- Discussions with the independent and internal auditors as to their views on the potential for fraud

Evaluation of Deficiencies

Because of the strong focus on fraud (¶¶24–26) and factors related to the effectiveness of the audit committee (¶¶57–59) in the PCAOB Proposed Auditing Standard, a passive attitude toward oversight and the topic of fraud and the antifraud programs and controls would be a strong indicator of a significant deficiency. The NYSE and NASDAQ rules also require active oversight by the board and audit committee.

Investigation/Remediation

One of the most critical aspects of a company's control environment, "tone at the top," and antifraud program is the way management, the audit committee and the board of directors respond to any significant deficiencies and material weaknesses that are identified in the antifraud program, and the way they respond to incidents of suspected, alleged or actual fraud. Paragraph 126 of the PCAOB Proposed Auditing Standard indicates that significant deficiencies that have been communicated to management and the audit committee and which remain uncorrected after some reasonable period of time become strong indicators of material weaknesses.

Sarbanes-Oxley §302 and the SEC's Final Rule entitled "Certification of Disclosure in Companies' Quarterly and Annual Reports" require, as part of the certification process, the principal executive officer(s) and principal financial officer(s) to disclose to the issuer's auditors and to the audit committee of the board of directors (or persons fulfilling the equivalent function):

- All significant deficiencies in the design or operation of internal controls that could adversely affect the issuer's ability to record, process, summarize and report financial data; and that they have identified for the issuer's auditors any material weaknesses in internal controls
- Any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls

Design and Documentation

The company must develop a standardized process for responding to allegations or suspicions of fraud. *It should not wait until fraud is detected to develop an investigative process.* Management, the audit committee and the board of directors must take appropriate actions to address identified significant deficiencies and material weaknesses of internal controls as well as any incidents of suspected, alleged or actual fraud that is material as well as fraud of any magnitude involving senior management. As applicable, the company's actions would generally include:

- Conducting a thorough investigation and assessment of the matter, potentially including a 10A investigation[4] by independent counsel
- Assessing and improving any relevant internal controls at the affected business unit, and, if appropriate, elsewhere in the organization
- Communicating and training to reinforce the entity's policies and procedures, values, code of conduct and expectations
- Taking appropriate and consistent actions against any violators
- Potentially communicating when wrongdoing occurs and an employee is disciplined, on a no-name basis, in an employee newsletter or other regular communication to employees
- Making appropriate disclosures in the company's periodic reports filed with the SEC

The company should create and maintain documentation of the process, proceedings and resolutions. Internal audit or an independent party working on behalf of the audit committee should conduct a walk-through of the process.

Operating Effectiveness

The question of what constitutes effective remediation is one of judgment and is often based to a large degree on hindsight. At the very least, the audit committee should ensure that appropriate and timely follow-up occurs. This assessment should include an examination of a sampling of incident investigations and remediation of alleged serious misconduct (as identified by management). Advice of counsel should be obtained for difficult decisions. Inquiries should be made and evidence examined to determine that significant deficiencies and material weaknesses previously identified have been remediated or that a good faith effort to do so is underway. Evidence of active audit committee involvement should be reflected in the audit committee minutes and in reports noting investigations and subsequent actions.

Evaluation of Deficiencies

A company's failure to 1) disclose significant deficiencies or fraud to the external auditor or its audit committee or 2) take appropriate remedial action with regard to identified significant deficiencies, material weaknesses, actual fraud or suspected fraud is a significant deficiency and a strong indicator of a material weakness as indicated in ¶126 of the PCAOB Proposed Auditing Standard.

---

4 The Private Securities Litigation Reform Act of 1995 (Public Law 104-67) added Section 10A to the Securities Exchange Act of 1934, 15 U.S.C. §78j-1. Section 10A requires a public company's board of directors or auditor to notify the SEC about possible illegal acts when, during the course of a financial audit, an auditor detects likely illegal acts that have a material impact on the financial statements and appropriate remedial action is not taken by management or the board of directors. See U.S. General Accounting Office, *Securities Exchange Act: Review of Reporting Under Section 10A* (September 3, 2003).

Fraud Risk Assessment

Organizations should consider the potential for fraud as part of their enterprise-wide risk assessment process or risk management program. Fraud risk assessment expands upon traditional risk assessment. It is scheme and scenario based rather than based on control risk or inherent risk. The assessment considers the various ways that fraud and misconduct can occur by and against the company. Fraud risk assessment also considers vulnerability to management override and potential schemes to circumvent existing control activities, which may require additional compensating control activities.

The fraud risk assessment process should consider vulnerability of the entity to fraud and its potential impact on financial statements. Sarbanes-Oxley §103 requires the independent auditor's evaluation of internal controls to address controls to ensure that "receipts and expenditures of issuers are being made only in accordance with authorization of management and the directors." The SEC's Final Rule refers to "unauthorized acquisition, use or disposition" of the organization's assets.

Management's assessment of fraud risk should include the potential for fraudulent financial reporting, misappropriation of assets, and unauthorized or improper receipts and expenditures. Management's assessment of fraud risk should also consider the risk of fraud by senior management or the board because "fraud of any magnitude on the part of senior management" constitutes a significant deficiency and is a strong indicator of a material weakness as stated in ¶126 of the PCAOB Proposed Auditing Standard. Additionally, in accordance with ¶36 of SAS 99, management's assessment of fraud risks should consider incentives and pressures on management to commit fraud.

To be effective, management should perform fraud risk assessments on a comprehensive and recurring basis rather than in an informal or haphazard manner. The COSO framework instructs that risk assessments should also occur when special circumstances arise, such as changed operating environments, new products and markets, and corporate restructurings. Management should include fraud risk in these assessments.

Management must also assess fraud risk at the company-wide, business unit and significant account levels. The nature and extent of management's risk assessment activities should be commensurate with the size of the entity and complexity of its operations (for example, the risk assessment process is likely to be less formal and less structured in smaller, centralized entities).

Design and Documentation

The essential elements of an effective fraud risk assessment include:

- Systematic (rather than haphazard) assessment process
- Consideration of potential fraud schemes and scenarios
- Assessment of risk at company-wide, significant business unit and significant account levels
- Evaluation of the likelihood and significance of each risk to the organization

• Assessment of exposure arising from each of the categories of fraud risk
• Testing of effectiveness of risk assessment process by internal audit
• Documented oversight by the audit committee, including consideration of the risk of override of controls by management

The audit committee and the board, in performing their fiduciary duties, are responsible for considering their own knowledge of the company's underlying performance, the types of fraud prevalent in the sector, the risk of financial fraud by management, and ensuring that controls or mitigating actions have been taken to prevent and detect fraud. The audit committee and the board should consider management's risk assessment processes, specifically including consideration of the following:

• Process for identifying and documenting fraud risk
• Types of fraud considered by management (fraudulent financial reporting, misappropriation of assets, unauthorized or improper receipts and expenditures, and fraud by senior management)
• Level at which risk is considered (company-wide, business unit and significant account)
• Level of likelihood of fraud (probable, reasonably possible and remote)
• Level of significance of fraud (inconsequential, more than inconsequential, material)

Organizations will need to reach their own conclusions with respect to the cost of controlling a risk compared to the benefits of mitigating or eliminating that risk. However, an organization should have a documented process that assesses, identifies and evaluates fraud risk.

In accordance with SAS 99, audit committees should have an open and candid dialogue with the independent auditors regarding management's risk assessment process and the system of internal controls, specifically including a discussion of:

• Susceptibility of the entity to fraudulent financial reporting
• Exposure to misappropriation of assets or unauthorized receipts and expenditures
• The committee's views about the risks of fraud and the risk of override of controls by management
• Whether the committee has any knowledge of suspected or actual fraud
• The nature of the committee's oversight activities in this area

Operating Effectiveness

Inasmuch as an effective risk assessment is a fluid process, there should be documentary evidence of periodic and systematic fraud risk assessment. Internal audit testing should be reviewed as well as the assessment of financial reporting risk. A fraud assessment by the audit committee and the discussion with the external auditor should be evidenced in the audit committee's meeting minutes.

Evaluation of Deficiencies

Given the critical importance of an effective risk assessment process to effective internal control over financial reporting and deterring and detecting fraud and suspected fraud as indicated in both ¶¶24 and 126 of the PCAOB Proposed Auditing Standard, the absence of adequate documentary evidence of management's risk assessment process and the audit committee's involvement and review is a strong indicator of a significant deficiency and may be an indicator of a material weakness.

Control Activities

Once the fraud risk assessment has taken place, the organization should identify the control activities implemented to mitigate the identified fraud risk. In the context of an antifraud management program, control activities are those actions taken by management to identify, prevent and mitigate fraudulent financial reporting or misuse of organizations' assets. Antifraud control activities should occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, segregation of duties, reviews of operating performance and security of assets.

Management should evaluate whether appropriate internal controls have been implemented in any areas management has identified as posing a higher risk of fraudulent activity (such as revenue recognition and non-standard journal entries), as well as controls over the entity's financial reporting process and the potential for management override. Because of the importance of information technology in supporting operations and the processing of transactions, management also needs to implement and maintain appropriate controls, whether automated or manual, over computer-generated information.

The environment in which an entity operates affects the fraud risks to which it is exposed and may present unique external reporting requirements, or special legal or regulatory requirements. An entity's antifraud program must consider whether the controls implemented are adequate to address all of the individual entity's specific business activities; whether these controls are properly designed for purposes of detecting, deterring and mitigating the particular fraud risks to which the entity is exposed; and whether these controls are being applied properly to sufficiently address the entity's unique business operations and fraud risks.

Design and Documentation

Management should design the necessary control activities to respond to the assessed fraud risks. The necessary control activities should be documented in a manner that will ensure that each of the significant fraud exposures identified during the risk assessment process have been adequately mitigated. This is generally done through a linking or mapping process of the business procedure, relating the risk of potential misstatement to the control activities and then to the relevant financial statement assertions. The audit committee should evidence their oversight and approval of the adequacy of the design and operating effectiveness of the control activities in minutes of their meetings. Internal audit or a third party working on behalf of the audit committee should evaluate the effectiveness of the design of control activities through a walk-through.

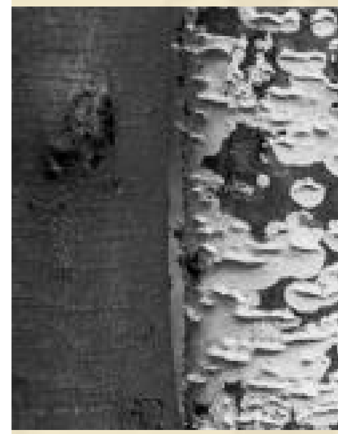
Operating Effectiveness

Testing of control activities should include any business process where there is an identified risk of fraud.

Evaluation of Deficiencies

The lack of an adequately designed, documented and tested system of control activities addressing each of the identified fraud risks is a strong indicator of a significant deficiency. Deficiencies in the control of specific frauds, whether individually or in the aggregate, should be evaluated to determine if they constitute a material weakness.

Information and Communication



Effective communication is critical to ensuring the success of antifraud programs and policies. Antifraud policies must be stated clearly and spell out each employee's responsibilities in relation to the program. This information must then be communicated to employees *effectively*; that is, in a form and time frame that allows employees to carry out their responsibilities. Thus, an assessment of the entity's antifraud program must consider whether the content of its policies is appropriate, timely, current and properly disseminated to all appropriate parties.

In order to be effective, communication regarding the company's antifraud policies and procedures must flow down, up and across an organization. All personnel must receive a clear message that the company is serious about its commitment to preventing fraud. In addition, each employee must fully understand all relevant aspects of the company's antifraud program and his or her role and responsibilities as they relate to following and enforcing the company's antifraud policies. Every employee needs to know what behavior is expected or acceptable, and what is unacceptable.

Employees must also have an effective means of communicating significant information relating to fraud upstream. Lastly, effective communication regarding the company's antifraud policies must also occur between the entity and external parties, such as customers, suppliers, regulators and shareholders.

Design and Documentation

A company must engage in effective knowledge management. With regard to fraud, that means being able to collect and share information regarding identified fraud risks, strengths and weaknesses of antifraud control activities, suspicions and allegations about fraud and remediation efforts. The company should consider using its information systems and technology as important tools in these efforts.

The company's information systems and technology overlay all five of the COSO components and are integral elements of an antifraud program. Further, information technology audits ordinarily cover many fraud-related issues such as access to system resources, authentication of data and the like.

With respect to information systems and technology, antifraud programs and controls should address:

- Consideration, in management's fraud risk assessment, of technologically enabled fraud such as manipulating system time clocks that affect cut-off on the books and records[5]
- IT security controls, with increased emphasis on prevention and detection of unauthorized access and physical intrusion
- Impact of system access on segregation of duties
- Adequacy of fraud detection and monitoring tools such as of fraud-related computer-assisted auditing techniques

The organization's computer environment and any automated controls to deter and detect fraud on a timely basis, including systems security, should be documented.

Operating Effectiveness

An evaluation of the effectiveness of the information gathering and communication of a company's antifraud program, beyond the procedures performed under "Control Environment" and "Risk Assessment," should include:

- Whether the company's code of conduct and antifraud policy statements are available on the company's website or appended to SEC filings
- Frequency and sufficiency of training provided to employees regarding how to identify ethical challenges and act responsibly
- Adequacy of capabilities to collect and share information about fraud across the organization
- The manner by which the company communicates the results of any investigation or disciplinary actions taken
- Inappropriate modifications to computer programs by IT personnel, such as falsification of financial reports
- System override of control features, such as using information systems to circumvent control activities
- Ability to investigate computer misuse, such as computer forensics/incident response capabilities and maintaining system logs for an adequate period to perform investigations

General computer controls related to security should be tested to ensure they are operating effectively.

---

5 Controls over program changes are a common problem area in financial statement fraud. A classic "fraud triangle," for example, would include: (1) *incentive*: programmer's compensation is rewarded by business unit, business unit compensation is rewarded by meeting revenue goals, (2) *opportunities*: weak program change controls allow developer access into production, and (3) *rationale*: programmer follows instructions and does not question the ethical merit of the business unit leader's change request – it is not their business.

Evaluation of Deficiencies

Inadequate training and communications and defective knowledge management may constitute a significant deficiency. The absence of training programs and communications and a lack of evidence of senior management's attention to collecting information regarding fraud are strong indicators of a significant deficiency.

Because of the pervasive effect of IT security and controls on information initiated, recorded, processed and reported, any weakness in this area provides significant opportunities for fraud and is therefore a strong indicator of a significant deficiency.

Monitoring

As is the case with all internal controls, a company's antifraud controls, programs and policies must be monitored, that is, subjected to ongoing and periodic performance assessments. The frequency of separate evaluations or audits necessary for management to have reasonable assurance about the effectiveness of its antifraud controls is a matter of management's judgment. In making that determination, consideration should be given to the following: the nature and degree of changes occurring in the entity and their associated risks, the competence and experience of the individuals implementing the controls, and the results of ongoing monitoring.

Information technology creates both risk and opportunity. The use of computer-assisted audit techniques can significantly enhance the effectiveness of an entity's monitoring activities. In addition, numerous software programs are available to allow organizations to search for and detect fraudulent activity.

Design and Documentation

Ongoing monitoring occurs in the course of operations and should be built into the normal, recurring operating activities of an enterprise. It includes regular management and supervisory activities and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of fraud risks and the effectiveness of ongoing monitoring procedures. Since separate evaluations occur after the fact, problems will be identified more quickly by ongoing monitoring routines.

Separate evaluations will ordinarily be conducted by the internal audit department or equivalent function. It is essential that the organization's plan, approach, and scope of monitoring activities be documented and reviewed from time to time. The oversight of the internal audit function is discussed in the "Control Environment" section.

Operating Effectiveness

In considering the extent to which the effectiveness of an entity's antifraud controls is monitored, both ongoing monitoring activities and separate evaluations of the internal control system, or portions thereof, should be considered.

An evaluation of management's monitoring systems should include evidence relating to the following:

- Management's responsibility for enforcement and monitoring of the antifraud program and policies
- Prompt and sufficient response to significant deficiencies and material internal control weaknesses
- Periodic comparisons of amounts recorded by the accounting system against physical assets
- Responsiveness to internal and external auditor recommendations regarding ways to strengthen antifraud controls

An evaluation of the internal audit function, in addition to the discussion in Control Environment, should address:

- Adequacy of the nature, extent, scope and effectiveness of internal audit activities relating to fraud. Although a determination of adequacy is a subjective one, the internal audit's plan should document their risk assessment, procedures and record of work performed. Rotational planning should include attention to company locations that might not be materially significant but are in locations with a higher risk of fraud.
- Knowledge and experience of individuals, and whether they receive periodic and adequate training with regard to fraud.

Evaluation of Deficiencies

Lack of a documented system of monitoring the effectiveness of the antifraud program and absence of routine fraud auditing in the scope of the internal audit (or equivalent) department's annual plan are both strong indicators of a significant deficiency.

III. Summary and Conclusion

The Whole Is Greater Than the Sum of Its Parts

The elements discussed above must all work together to form an effective antifraud program, and thus should be considered in the aggregate as an integrated system. The absence of multiple elements should raise a concern about the adequacy of the program or a COSO control component. Any deficiencies should also be evaluated in the aggregate to consider whether they combine in a way that creates a significant deficiency and whether significant deficiencies when aggregated become a material weakness.

One Size Does Not Fit All

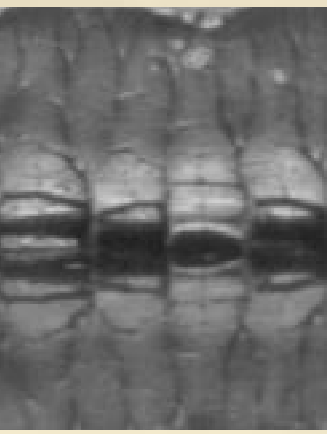
Most entities should have formal documentation of their antifraud programs. The only exception is the case of the smaller, centralized organization where the importance of and emphasis on integrity and ethical behavior is exhibited via visible and direct involvement of the CEO and top management in employee meetings, dealings with customers and vendors, and so forth. In such situations, the lack of a documented and effectively communicated code of conduct may not adversely affect the effectiveness of the control environment. Such exceptions with regard to documentation are generally only appropriate for entities with 50 or fewer employees and with only one location. However, in all cases the direct involvement of senior management should be confirmed. This can be best accomplished through walkabouts — essentially corroborating through inquiries of employees and by making calls to customers and vendors.

Appropriate Treatment

Fraud can easily spread from a small brush fire into a full-blown firestorm. Yet with proper techniques and readiness companies can, if not avoid fraud altogether, at least identify it early and minimize the damage that it causes. Companies that establish antifraud programs as described above will meet compliance requirements. More important, however, they will go a long way toward meeting their shareholders' expectations and helping to restore confidence in the financial markets. Finally, fraud management makes good business sense. Fraud prevention and detection create large cost savings that go directly to the bottom line and can significantly improve the company's financial performance.

Appendix A:
Highlights of Antifraud Laws, Regulations and Standards

Authority	Date	Provisions
United States Sentencing Commission[1] (referred to as USSC)	Nov. ’91	• Introduced seven criteria for “effective” management of ethics and compliance risk, which have emerged as the benchmark of an effective compliance program.[2] • No mandatory third-party evaluation; program evaluated only if company is seeking to mitigate penalties for corporate misconduct.



1 U.S. Sentencing Guidelines Manual Chapter 8 (November 2002) available at: http://www.ussc.gov/2002guid/tabconchapt8.htm [hereinafter USSG].

2 The seven criteria are:

1) The organization must have established compliance standards and procedures to be followed by its employees and other agents that are reasonably capable of reducing the prospect of criminal conduct.
2) Specific individual(s) within high-level personnel of the organization must have been assigned overall responsibility to oversee compliance with such standards and procedures.
3) The organization must have used due care not to delegate substantial discretionary authority to individuals who the organization knew, or should have known through the exercise of due diligence, had a propensity to engage in illegal activities.
4) The organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents, e.g., by requiring participation in training programs or by disseminating publications that explain in a practical manner what is required.
5) The organization must have taken reasonable steps to achieve compliance with its standards, e.g., by utilizing monitoring and auditing systems reasonably designed to detect criminal conduct by its employees and other agents and by having in place and publicizing a reporting system that can be used by employees and other agents to report criminal conduct of others within the organization without fear of retribution.
6) The standards must have been consistently enforced through appropriate disciplinary mechanisms, including, as appropriate, discipline of individuals responsible for the failure to detect an offense. Adequate discipline of individuals directly responsible for an offense is a necessary component of enforcement; however, the form of discipline that will be appropriate will be case specific.
7) After an offense has been detected, the organization must have taken all reasonable steps to respond appropriately to the offense and to prevent further similar offenses — including any necessary modifications to its program to prevent and detect violations of law.

Authority	Date	Provisions
		• The USSC appointed an Ad Hoc Advisory Group, which, in October 2003, recommended additional requirements to the seven criteria.[3]
The Sarbanes-Oxley Act of 2002[4] §§ 103, 404 (referred to as Sarbanes-Oxley or Section 404)	July '02	• Section 103: "receipts and expenditures of issuers…in accordance with authorization of management and the directors." • Section 404: requires management to assert to the effectiveness of internal controls over financial reporting.
Statement on Auditing Standards, "Consideration of Fraud in a Financial Audit"[5] now a part of the PCAOB's Interim Standards (Referred to as SAS 99)	Oct. '02	• Applies to financial statement audit of both registrants and non-registrants. • Requires the auditor to (1) identify risks that may result in a material misstatement due to fraud, (2) assess the identified risks after taking into account an evaluation of the entity's programs and controls and (3) respond to the results of the assessment, including, but not limited to changing: – The overall approach to the audit – The nature, timing and extent of specific auditing procedures to be performed – Procedures to address the risk of management override of controls

3 For the Executive Summary, Table of Contents or entire report, see the web link at http://www.ussc.gov/corp/advgrp.htm. The additional criteria include:
1) The company must promote a culture of compliance with law.
2) Senior and mid-level management must be knowledgeable about the program.
3) The board must be knowledgeable about the program and provide reasonable oversight.
4) High-level persons must report on implementation and effectiveness to the board.
5) The company must train the board, management, other employees and, as appropriate, agents.
6) The system must also provide a way for employees to "seek guidance" on issues.
7) Periodic evaluation of the compliance program is required.
8) The compliance program must be promoted through appropriate incentives to "perform in accordance with" the compliance program.
9) The company must engage in ongoing risk assessment and design and implement and modify the compliance program in light of information from risk assessments.
10) Risk assessment includes prioritization based on likelihood and seriousness of risk.
See "BNA Prevention of Corporate Liability, Ad Hoc Advisory Group Recommends Changes to Federal Sentencing Guidelines for Organizations" (November 2003).

4 Sarbanes-Oxley Act of 2002, 15 U.S.C. §7201 (2002)

5 Auditing Standards Board, Statement on Auditing Standards, "Consideration of Fraud in a Financial Statement Audit" (October 2002) [hereinafter "SAS 99"].

Authority	Date	Provisions
		• Attaches an exhibit co-authored by numerous associations entitled "Management Antifraud Programs and Controls," which provides examples of programs and controls an entity may implement to prevent, deter and detect fraud.
SEC's Final Rule for Section 404 of Sarbanes-Oxley, "Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Period Reports"[6] (referred to as SEC Final Rule)	June '03	• Refers to "unauthorized acquisition, use or disposition" of the organization's assets. • Requires management to assess the design and operating effectiveness of its company's internal control over financial reporting. • Controls subject to mandatory management assessment expressly include controls related to the prevention, identification and detection of fraud.
Public Company Accounting Oversight Board (PCAOB) Proposed Auditing Standard[7]	Oct. '03	• Requires the auditor to evaluate all controls over risks of fraud that are reasonably likely to have a material effect on the company's financial statements, including, but not limited to: – Inappropriate use of company assets – Risk assessment – Codes of ethics/conduct – Adequacy of internal audit – Adequacy of procedures for handling complaints • Evaluation must address both the design and operating effectiveness of such programs and controls.

6 See Final Rule: Management's Report on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports, Securities and Exchange Commission Release No. 33-8238 (June 5, 2003) [68 FR 36636].

7 Proposed Auditing Standard – *An Audit of Internal Control Over Financial Reporting Performed In Conjunction With An Audit of Financial Statements*, Public Company Accounting Oversight Board Release No. 2003-017 (October 7, 2003) [hereinafter "PCAOB"].

Authority	Date	Provisions
		• Mandates “at least a significant deficiency” and is a “strong indicator” of a material weakness, if: – Fraud by senior management of “any magnitude” is identified – Internal audit or risk assessment function is ineffective in a large, complex entity – A regulatory compliance function is ineffective in complex entities in regulated industries
NYSE Corporate Governance Proposal, as amended, and various NASDAQ proposals, as amended[8] approved by SEC (referred to as Listing Markets)	Nov. ’03	• Proposals are “consistent with the Exchange Act and the rules and regulations promulgated thereunder applicable to a national securities exchange and, in particular, with the requirements of Section 6(b) of the Exchange Act.” • “Specifically, the Commission finds that the NYSE Corporate Governance Proposal, as amended, is consistent with Section 6(b)(5) of the Exchange Act in that it is designed, among other things, to facilitate transactions in securities; *to prevent fraudulent and manipulative acts and practices…”* [emphasis added].

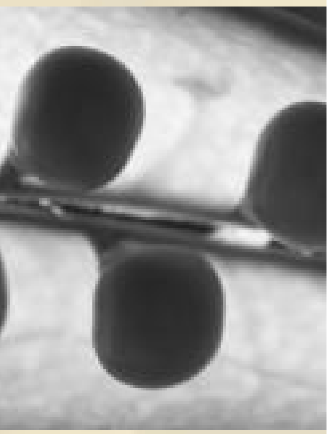
8 On Nov 4, 2003 the SEC approved the New York Stock Exchange, Inc. (“NYSE” or “Exchange”) proposed rule change (SR-NYSE-2002-33, August 16, 2002), as amended by NYSE Amendment No. 1, (April 4, 2003), and the NASDAQ Independent Director Proposal (SR-NASD-2002-141, October 9, 2002), as amended; the NASDAQ Going Concern Proposal (changes SR-NASD-2002-77); the NASDAQ Related Party Transactions Proposal (SR-NASD-2002-80 as amended; the NASDAQ Issuer Applicability Proposal (SR-NASD-2002-138), as amended; and the NASDAQ Code of Conduct Proposal (SR-NASD-2002-139).

Appendix B:

Definitions of Significant Deficiency and Material Weakness

Under Section 404, management must assess the likelihood of a potential misstatement even though an actual misstatement may not have occurred.

The PCAOB proposed auditing standard states that internal control deficiencies exist when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. These deficiencies can range from inconsequential internal control deficiencies to material weaknesses in internal control:



- **Inconsequential** – The identified exceptions are deemed negligible or insignificant, individually. However, two or more individually inconsequential control deficiencies, when considered in the aggregate (for example, multiple deficiencies common to a specific account or business unit), may constitute a significant deficiency.

- **Significant deficiency** – An internal control deficiency that adversely affects the company's ability to initiate, record, process or report information in its external financial statements in accordance with generally accepted accounting principles. A significant deficiency is a single deficiency, or a combination of deficiencies, that results in more than a remote likelihood that a misstatement of the financial statements that is more than inconsequential in amount will not be prevented or detected.

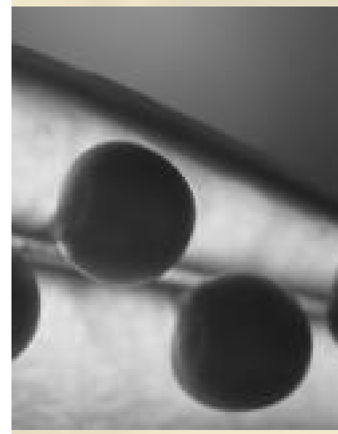
- **Material weakness** – A significant deficiency that, by itself, or in combination with other significant deficiencies, results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

Appendix C:
Table of Indicators of Significant Deficiencies

Knowing what the "minimum requirements" are is difficult because the programs and controls must be looked at as a whole. Following is a list of circumstances, which, in and of themselves, are strong indicators of significant deficiencies.

COSO Component	Strong Indicator of Significant Deficiency	Authoritative References
Control Environment		
Management Accountability	Senior management conducts ineffective oversight of antifraud programs and controls.	Sarbanes-Oxley §404 SEC Final Rules PCAOB ¶¶19, 24, 41, 128, 148 USSG Chap. 8
Audit committee	Audit committee passively conducts oversight. It does not actively engage the topic of fraud.	SAS 99 (Exhibit) COSO Chap. 8 PCAOB ¶¶24, 57, 59 SAS 99 (Exhibit) COSO Ch. 2 Sarbanes-Oxley §406
Code of Conduct/Ethics	Non-existent code or code that fails to address conflicts of interest, related party transactions, illegal acts, and monitoring by management and the board. Ineffective communication to all covered persons.	SEC Final Rules PCAOB ¶24 USSG Ch. 8 COSO Ch. 2
Hotlines	Whistleblower program significantly defective in design or operation.	Sarbanes-Oxley §301 SEC Rules for Audit committees §IIC[1] PCAOB ¶24 USSG Ch. 8
Hiring and Promotion Procedures	Failure to perform substantive background investigations for individuals being considered for employment or promotion to a position of trust.	PCAOB ¶24 USSG Ch. 8

1 Standards Related to Listed Company Audit Committees, Securities and Exchange Commission Release Nos. 33-8220, 34-47654 (April 25, 2003).



COSO Component	Strong Indicator of Significant Deficiency	Authoritative References
Investigative Process	Inadequate process for responding to allegations of suspicions of fraud.	USSG Ch. 8 COSO Ch. 2
Remediation	Failure to take appropriate and consistent remedial action with regard to identified significant deficiencies, material weaknesses, actual fraud or suspected fraud.	
Risk Assessment Process for Assessing Risk	Assessment of fraud risk is not systematic but rather informal and haphazard.	PCAOB ¶¶24, 50 SAS 99 (Exhibit) COSO Ch. 3
Frauds Considered	Management does not consider risks of fraudulent financial reporting, misappropriation of assets, unauthorized receipts and disbursements, and fraud by senior management.	Sarbanes-Oxley §103 SEC Final Rules§IIA3 PCAOB ¶¶6, 24, 126, 128, Appendix C SAS 99 ¶5
Likelihood and Significance of Fraud	Management's risk assessment process does not identify the likelihood and significance considered. Management should provide an explanation if its risk assessment process does not consider risks that are (1) reasonably possible and material, (2) probable and more than inconsequential in amount, and (3) reasonably possible and more than inconsequential in amount.	PCAOB ¶¶8, 119–123 SAS 99 ¶40 COSO Ch. 3
Level Within Organization	Management does not consider significant business units or significant processes in the fraud risk assessment.	PCAOB ¶¶55, 60–71, Appendix B SAS 99 ¶38 COSO Ch. 2
Risk of Management Override	Company (including audit committee) does not adequately consider the risk of management override.	PCAOB ¶140 SAS 99 ¶42

COSO Component	Strong Indicator of Significant Deficiency	Authoritative References
Control Activities Linkage with risk assessment	Management cannot map specific control activities to identified risks.	PCAOB ¶¶43–46, 50 SAS 99 ¶¶44–45 SAS 99 (Exhibit) COSO Ch. 4
Information and Communication Training	Training regarding code of ethics and other fraud areas is nonexistent or ineffective.	PCAOB ¶50 SAS 99 (Exhibit) USSG Ch. 8
Knowledge Management	Collecting and sharing of information regarding fraud risks, controls activities and remediation of identified misconduct are either non-existent or seriously defective.	PCAOB ¶50 USSG Ch. 8 COSO Ch. 5
Information Systems & Technology	Management fails to (1) consider information technology in fraud risk assessment, (2) maintain adequate security and access controls, (3) employ information technology to prevent and detect fraud or (4) have an ability to investigate computer misuse.	
Monitoring Monitoring by Management	Management does not consider possibility of fraud in its day-to-day operations.	PCAOB ¶¶24, 50 USSG Ch. 8 SAS 99 Appendix A COSO Ch. 6
Internal Audit Evaluations	Internal audit does not adequately address fraud risk in planning and executing the annual audit cycle.	PCAOB ¶¶24, 126 SAS 99 Appendix A
	Internal audit department fails to include knowledgeable and experienced fraud professionals.	PCAOB ¶¶24, 126 IIA Standards §1210.A2[2] IIA Practice Advisory[3]

2 Institute of Internal Auditors, International Standards for the Professional Practice of Internal Auditing.
3 Institute of Internal Auditors, Practice Advisory 1210.A2-1: Identification of Fraud.

Quick Reference Guide to Key Actions to Consider

Although most public companies already have components of an antifraud program in place (e.g., codes of ethics and conduct), companies likely will need to undertake supplemental actions to avoid significant deficiencies or material weaknesses. Following are the areas likely to require supplemental action.

Element	Common Practice Today	Key Actions
Board and Audit Committee Oversight	Passive oversight	Active oversight of fraud risk assessment process and antifraud measures. Functional responsibility and interaction with internal and external audit regarding fraud.
Scope of "Fraud"	No common definition	Broadly defined to include (1) fraudulent financial reporting and (2) unauthorized acquisition, use and disposition of assets.
Investigation and Remediation	Unstructured	Implement standardized process for responding to allegations or suspicions of fraud. Document efforts to take appropriate and consistent action against violators, improve controls and institute other actions to prevent recurrence.
Fraud Risk Assessment	Rarely performed	Systematic and ongoing fraud risk assessment process that is (1) conducted at business unit and significant account levels and (2) identifies fraud risks that are more than remote and more than inconsequential in amount. Fraud risk assessment is scheme and scenario based rather than based on control risk or inherent risk. Fraud risk assessment also considers vulnerability to management override and potential schemes to circumvent existing control activities.

Element	Common Practice Today	Key Actions
Linking Control Activities To Identified Fraud Risks	Rarely performed	Identify the processes, controls and other procedures that are needed to mitigate the identified risks.
Fraud Monitoring	Rarely performed	Develop ongoing monitoring for fraud into the normal, recurring operating activities.
Fraud Auditing	Rarely performed	Address fraud risk in planning and executing the annual internal audit cycle. Obtain fraud training for internal audit staff.
Knowledge Management	Rarely performed	Share information about fraud risks, antifraud control activities, allegations and remediation efforts. Use software tools.

About PricewaterhouseCoopers

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services for public and private clients. More than 120,000 people in 139 countries connect their thinking, experience and solutions to build public trust and enhance value for clients and their stakeholders.

www.pwc.com