



Prevention of Corporate Liability

C U R R E N T R E P O R T

Reproduced with permission from Prevention of Corporate Liability, Vol. 12, No. 03, 4/19/2004. Copyright © 2004 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

A New Audience for COSO—SEC & PCAOB Requirements for Anti-Fraud Programs & Control

BY JONNY FRANK & NANCY NEWMAN-LIMATA

Companies subject to the Sarbanes-Oxley Act¹ must now implement “anti-fraud programs and controls”.² Seemingly innocuous, this new requirement creates new responsibilities for many not previously involved in internal control over financial reporting, particularly for in-house counsel and

Jonny Frank and Nancy Newman-Limata are members of PricewaterhouseCoopers LLP. Ms. Newman-Limata is a partner in the firm’s National Risk & Quality Group. Mr. Frank is also a partner and leads the Fraud Risks & Controls practice at PricewaterhouseCoopers LLP and serves on the faculties of the Yale School of Management, Fordham University School of Law, and Brooklyn Law School. He previously served as the Executive Assistant United States Attorney of the Eastern District of New York. The views expressed in this article are their own and do not represent that of PricewaterhouseCoopers LLP.

¹ Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7201 (2002) (Sarbanes).

² For an in-depth discussion, see PricewaterhouseCoopers *Key Elements of Antifraud Programs and Controls*, available at www.dfodirect.com/News and Analysis/Corporate Governance/Key Elements of Antifraud Programs and Controls (December 2003).

compliance and ethics officers, who must become conversant with new terms, such as “COSO”, “PCAOB Auditing Standard No. 2”, and “internal controls over financial reporting”.

Most companies have elements of an anti-fraud program, as there is substantial overlap with United States Sentencing Guidelines (FSG)³ based compliance programs. While a code of conduct and ethics hotline/whistleblower program are familiar elements of such a program, elements that are likely to be less familiar to compliance professionals include (1) active audit committee oversight, (2) an effective fraud risk assessment, (3) adequacy of internal audit activities relative to prevention and detection and fraud, and (4) sufficiency of procedures for handling complaints and the reporting of fraud to the audit committee and independent auditor.⁴

³ U.S. Sentencing Guidelines Manual Chapter 8 available at <http://www.usssc.gov>.

⁴ Public Company Accounting Oversight Board (PCAOB), “An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements” (hereinafter PCAOB Auditing Standard No. 2) ¶ 24 (PCAOB Release No. 2004-001, dated March 9, 2004).

What happens when fraud occurs after management asserts that its internal controls are effective? Does this potentially give rise to an additional cause of action? Prosecutors, regulators, and private litigants likely will seek to hold a company liable for asserting to the effectiveness of controls that subsequently were demonstrated to be ineffective.

Shift From FSG to COSO

Companies historically viewed fraud prevention as an *implicit* facet of compliance activities as opposed to part of an *explicit* component of internal controls. With a compliance-driven approach, the FSG serve as the primary benchmark of effectiveness. The FSG are reactive: they address punitive implications *after* an occurrence of fraud or another form of corporate misconduct. A negative event of this sort is typically the impetus for an external party (usually lawyers) to evaluate and test the effectiveness of an FSG-based compliance program. Furthermore, the objectives around fraud prevention are different and internal control over financial reporting emphasizes the importance of the control environment of the organization in setting the “tone at the top.”

Now, however, control factors are rapidly replacing compliance concerns as the primary drivers of anti-fraud programs. Today's marketplace and regulatory environment demand proactive anti-fraud programs characterized by a strong focus on the prevention and timely detection of fraud.

Sarbanes requires management to assert to the effectiveness of internal controls over financial reporting. The SEC's final rules implementing Sarbanes refer explicitly to controls related to the *prevention, identification, and detection* of fraud.⁵ The regulations require corporate management to evaluate and test the design and operating effectiveness of anti-fraud controls on an annual basis.⁶ Management is required to identify fraud

(continued on page 32)

(continued from page 36)

by senior management, regardless of how immaterial. The goal is to ensure that controls are in place to address management overrides. Independent auditors will evaluate and test their designs and operating effectiveness as a part of the integrated audit.⁷ PCAOB auditing standards provide deficient anti-fraud programs and controls "ordinarily results" in a finding of at least a significant deficiency.⁸ Management cannot assert that they have effective internal control over financial reporting if any deficiency rises to a material weakness. Furthermore, the auditor must issue an adverse opinion if it concludes that any deficiency or aggregation of deficiencies rise to a material weakness.⁹

COSO = FSG+

In the United States, the Committee of Sponsoring Organizations (COSO) of the Treadway Commission has emerged as the framework that management and auditors use to evaluate internal controls.¹⁰ COSO expands upon existing FSG requirements.¹¹ The FSG, which were drafted by lawyers, emphasize governance and "softer" elements, such as training, communica-

⁵ U.S. Securities and Exchange Commission, "Management's Report on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports," Release No. 33-8328 (June 5, 2003) [68 FR 36636].

⁶ According to the rule, "Controls subject to such assessment include, but are not limited to . . . controls related to the prevention, identification, and detection of fraud. The nature of a company's testing activities will largely depend on the circumstances of the company and the significance of the control. However, inquiry alone generally will not provide an adequate basis for management's assessment [footnote omitted]."

⁷ Public Company Accounting Oversight Board (PCAOB), "An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements" (PCAOB Auditing Standard No. 2 ¶¶ 88-107) (PCAOB Release No. 2004-001, dated March 9, 2004).

⁸ PCAOB Auditing Standard No. 2 ¶ 139.

⁹ PCAOB Auditing Standard No. 2 ¶ 175.

¹⁰ Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control—Integrated Framework (COSO)*.

¹¹ In December 2003, the United States Sentencing Commission proposed far-reaching changes that would narrow the differences between the FSG and COSO. Specifically, the proposed amendments provide for companies to conduct ongoing risk assessments to form the basis for continuous improvement.

tions, and delegation of authority. COSO considers these same issues under "control environment," and places additional emphasis on risk assessments, controls, and monitoring and auditing.

COSO has five key components—*control environment, risk assessment, control activities, information, and communications and monitoring*.¹² PCAOB Auditing Standards require independent auditors to include anti-fraud programs and controls when evaluating the design and operating effectiveness of each of these components of internal control over financial reporting.¹³

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 savings¹⁴ opportunities, which directly affect the bottom line.

Control Environment

The control environment refers to such intangibles as integrity, ethical values, 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.

Compliance specialists, ethics officers, and in-house counsel are generally already familiar with most anti-fraud components of the control environment, as the FSG address similar issues:

- Requirement for a code of conduct/ethics¹⁵
- Whistleblower hotlines¹⁶
- Hiring and promotion¹⁷

¹² The COSO framework typically is presented as a cube with these five elements overlaying against financial reporting, compliance, and operational controls. Fraud cuts across all three elements, as fraud usually impacts the financial statement, the organization's compliance program, and operations.

¹³ PCAOB Auditing Standard No. 2 ¶ 24.

¹⁴ The Association of Certified Fraud Examiners (ACFE) projects that (1) the average company loses the equivalent of 6 percent of its revenue to fraud and (2) fraud accounts for \$60 billion in losses annually. ACFE, "2002 Report to the Nation, Occupational Fraud and Abuse."

¹⁵ Sarbanes § 406 and the SEC's Final Rule, titled "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.

¹⁶ Sarbanes § 301, the SEC's final rule titled "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: (i) receiving and retaining information about and treating alleged incidents involving the issuer regarding accounting, internal accounting controls, or auditing matters, and (ii) the confidential, anonymous submission of concerns by employees about questionable accounting or auditing matters.

¹⁷ Establishing standards for hiring and promoting the most qualified individuals, with emphasis on educational background, prior work experience, past accomplishments, and

- Remediation of identified incidents of fraud¹⁸

The FSG do not specifically consider active governance and oversight by the audit committee and board, which is a key component of the control environment. The audit committee has responsibility for assessing the risk of financial fraud by management and ensuring controls are in place to prevent, deter, and detect fraud by management. Their evaluation should consider:

- Management's anti-fraud programs and controls, including management's identification of fraud risks and implementation of anti-fraud measures,

- 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,

- Internal audit consideration of 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 their attention, and

- Functional reporting by internal and external auditors to the board and audit committee.

Because of the strong focus on fraud¹⁹ and factors related to the effectiveness of the audit committee²⁰ in the PCAOB auditing standards, a passive attitude toward oversight and the topic of fraud and the anti-fraud 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.

Fraud Risk Assessment

How can management develop anti-fraud controls without first identifying its fraud risks? Yet, prior to Sarbanes, few companies assessed fraud risk on a comprehensive and recurring basis rather than in an informal or haphazard manner.²¹

evidence of integrity and ethical behavior, demonstrate an entity's commitment to competent and trustworthy people. 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. This is consistent with the FSG criteria that the organization use "due care not to delegate substantial discretionary authority to individuals who the organization knew, or should have known though the exercise of due diligence, had a propensity to engage in illegal activities."

¹⁸ The FSG provide that "[a]fter 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."

¹⁹ PCAOB Auditing Standard No. 2 ¶¶ 24 – 26.

²⁰ PCAOB Auditing Standard No. 2 ¶¶ 55 – 29.

²¹ For an in-depth discussion of fraud risk assessment process, see PricewaterhouseCoopers, "The Emerging Role of Internal Audit in Mitigating Fraud and Reputation Risks" (March 2004), available at www.pwc.com.

A fraud risk assessment process, performed independently or integrated with the enterprise risk-assessment process, is a cornerstone of an anti-fraud program that anticipates, rather than reacts to, fraud and misconduct. The proposed amendments to the FSG likewise recognize the need for the risk-assessment process. An effective fraud and reputation-risk assessment may identify previously unidentified risks and strengthen the ability of the organization to prevent and detect fraud and misconduct before they emerge into a corporate embarrassment.

Fraud risk assessment expands upon traditional risk assessment. It can be 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 focus is how fraud can be perpetrated and then concealed.

Frauds Considered

Management's assessment of fraud risk should include the potential for (1) fraudulent financial reporting, (2) misappropriation of assets, and (3) unauthorized or improper receipts and expenditures. Management's assessment of fraud risk should also consider (4) 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.²²

Organizing The Assessment

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 the complexity of its operations (for example, the risk-assessment process is likely to be less formal and less structured in smaller, centralized entities).

The fraud risk-assessment process can be integrated with the company's general risk-assessment process or conducted as a separate exercise. Management can organize the assessment around the company's existing business cycles or establish a separate cycle for this purpose. Organizing around existing business cycles simplifies the process, except that the process can miss fraud risks that do not fit neatly within a particular business cycle.

Some companies prefer to create a separate cycle focused on fraud and reputation risk.

Identifying Potential Schemes and Scenarios

Identifying potential fraud schemes and scenarios for a company is a formidable challenge. Fraud schemes and scenarios differ drastically by product and service sector and geography. For example, sales and marketing schemes are quite common in the Asian market, whereas procurement fraud is more widespread in Central and South America. On the other hand, the types of schemes affecting a bank will differ from those

²² PCAOB Auditing Standard No. 2 ¶ 140.

affecting a manufacturer. While both companies may be obtaining assets in a fraudulent manner, the bank might do so by failing to credit interest or by charging improper fees, whereas the manufacturer may be shortshipping a distributor to obtain assets fraudulently.

The typical large multinational company thus faces hundreds of fraud risks. Developing scheme descriptions for the organization requires a deep knowledge of the industry or industries in which the organization operates, and the geographies in which business is conducted. The risk-assessment team should also include fraud risk and control experts, who understand (1) the technicalities and mechanics of potential fraud schemes, (2) scheme indicia, (3) what controls are available to prevent and detect the scheme, and (4) how to detect the fraud in the normal course of business. For this reason, internal audit is likely to be a prominent player.

Likelihood

Fraud risk assessments, like traditional risk assessments, consider the likelihood that a particular fraud will occur. PCAOB auditing standards refer to “remote”, “more than remote”, and “probable” in evaluating deficiencies.²³ An organization is required to address risks that could result in a material misstatement of the financial statements. However, once it is identified, management must address a deficiency that has “more than a remote” likelihood of occurring. Fraud risks deemed to be remote can be ignored, although it is advisable for the assessment team to document that the organization had considered the deficiency and why it has determined it to be remote.

Significance and Impact Upon Financial Statements

The assessment then addresses the significance of all deficiencies that are more than remote. In this context, PCAOB auditing standards refer to “inconsequential”, “more than inconsequential”, and “material”. PCAOB defines inconsequential as a misstatement that a reasonable person, “after considering the possibility of further undetected misstatements,” would find to “clearly be immaterial to the financial statements.”²⁴ The standard further provides, “If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement is more than inconsequential.”

Be careful about the term “material”. In this context, materiality refers to the significance of an item to the users of a set of financial statements.²⁵ SEC registrants

²³ PCAOB Auditing Standard No. 2 refers to Financial Accounting Standards Board Statement No. 5, *Accounting for Contingencies* (FAS No. 5), which uses the terms probable, reasonably possible, and remote. The PCAOB defines “more than remote” as reasonably possible or probable.

²⁴ PCAOB Auditing Standard No. 2 ¶ 9.

²⁵ Financial Accounting Standards Board (“FASB”) Statement of Financial Accounting Concepts No. 2, *Qualitative Characteristics of Accounting Information* (“CON 2”) describes materiality as “[t]he omission or misstatement of an item in a financial report is material if, in light of surrounding circumstances, the magnitude of the item is such that it is probable that the judgment of a reasonable person relying upon the report would have been changed or influenced by the inclusion or correction of the item.”

should note that SEC Staff Accounting Bulletin (SAB) 99, which provides guidance in determining materiality when fraud is discovered,²⁶ expands the frequently used rule of thumb that a misstatement or omission that is 5 percent of some factor (e.g., net income or net assets) is material to also address “qualitative” aspects of the particular matter being analyzed beyond the “quantitative” evaluation.

Fraud rises to the level of material if a reasonable person—say a shareholder or lender—would consider it important. When evaluating significance, management should consider the impact of the fraud scheme individually and in the aggregate. Some frauds, such as travel and expense fraud, might be inconsequential on an individual basis but be significant on a combined basis.

Control Activities

Management’s Responsibility

Next, management should identify and test the control activities that mitigate those fraud and reputation risks, focusing on those controls that if ineffective could have a more than remote likelihood of resulting in a material misstatement and have a more than inconsequential impact upon the financial statements.²⁷ As a rule of thumb, anti-fraud controls generally include controls designed to *prevent* fraud and those designed to *detect* fraud in a timely fashion when it occurs.²⁸ Management should expect to be able to link most identified fraud risks to existing control activities such as approvals, authorizations, verifications, reconciliations, segregation of duties, reviews of operating performance, and security of assets. Anti-fraud control activities should occur throughout the organization, at all levels and in all functions.

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 has 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. Management’s documentation should also identify the individuals who perform the controls and the consideration of segregation of duties.²⁹ It must also describe any material fraud and any other fraud, although not material, involving senior management or management or other employees who have a significant role in the company’s internal control over financial reporting.³⁰ Inadequate documentation of the anti-fraud control activities in and of itself can be a deficiency.

Management also needs to evaluate and test the design and operating effectiveness of anti-fraud con-

²⁶ 17 Code of Federal Regulations Part 211, August 12, 1999.

²⁷ PCAOB Auditing Standard No. 2 ¶ 9 defines “significant deficiency” as a control deficiency for which “there is more than a remote likelihood that a misstatement of the company’s annual or interim financial statements that is more than inconsequential will not be prevented or detected.”

²⁸ PCAOB Auditing Standard No. 2 ¶ 11.

²⁹ PCAOB Auditing Standard No. 2 ¶ 42.

³⁰ PCAOB Auditing Standard No. 2 ¶ 142.

trols.³¹ Management must conduct its own evaluation and testing of design and operating effectiveness. It cannot rely upon the independent auditor's evaluation and testing of its anti-fraud programs and controls. (Nor can the independent auditor's evaluation rely upon management's evaluation and testing.³²) The company faces a possible qualified or adverse opinion if it fails to conduct and document an adequate assessment.³³

Auditor Responsibility

The PCAOB auditing standards assign several responsibilities to the independent auditor. First, the independent auditor must understand and evaluate management's process for assessing the effectiveness of anti-fraud programs and controls.³⁴ Second, it must evaluate and test design and operating effectiveness of "all controls specifically intended to address the risks of fraud that have at least a reasonably possible likelihood of having a material effect on the company's financial statements," which specifically includes, but is not limited to: (i) misappropriation of assets, (ii) risk assessment of process, (iii) adequacy of internal audit function and its interaction with audit committee, (iv) codes of ethics, and (v) whistleblower and hotline procedures.³⁵ Third, the independent auditor must "evaluate fraud of any magnitude (including fraud resulting in immaterial misstatements) on the part of senior management. . . ."³⁶ The standards define "senior management" as the principal executive and financial officers signing the company's certifications as required under Section 302 of the Act as well as any other member of management who plays a significant role in the company's financial reporting process. Further, the standards note that the independent auditor should alter the nature, timing, and extent of audit procedures in light of evaluation of anti-fraud programs and controls.³⁷

Evaluation Process

Evaluation and testing of design and operating effectiveness includes all five COSO components of anti-fraud programs and controls.³⁸ PCAOB Auditing Standard No. 2 defines generally the process for evaluating and testing controls. When evaluating anti-fraud controls, management needs to address the possibility that individuals might seek to circumvent or override controls intended to prevent or detect fraud. The audit committee should evidence its evaluation of the adequacy of the design and operating effectiveness of the control activities in minutes of its meetings.

Information and Communication

As with the anti-fraud elements of the control environment component of COSO, ethics and compliance officers are generally familiar with the requirements of information and communication, as the FSG address

these same topics.³⁹ Anti-fraud 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 anti-fraud 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 anti-fraud 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 anti-fraud program and his or her role and responsibilities as they relate to following and enforcing the company's anti-fraud 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. Finally, effective communication regarding the company's anti-fraud policies must also occur between the entity and external parties, such as customers, suppliers, regulators, and shareholders.

The company's information systems and technology overlay all five components of COSO, but are considered part of the information and communication component. Information technology audits should be performed by internal audit and cover many fraud-related issues such as systems resources, authentication of data, and unauthorized access and physical intrusion.

Monitoring and Auditing

Both the FSG and COSO emphasize the need for monitoring. The FSG require "reasonable steps to achieve compliance with its standards" including "monitoring and auditing systems." The PCAOB Auditing Standards refer explicitly to adequacy of the internal audit function as a control related to fraud.⁴⁰

Under COSO, a company's anti-fraud controls, programs, and policies likewise must be monitored, that is, subjected to ongoing and periodic performance assessments. 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 regularly.

³⁹ The FSG criteria include that the "organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents. . . ."

⁴⁰ PCAOB Auditing Standard No. 2 ¶ 24.

³¹ PCAOB Auditing Standard No. 2 ¶¶ 40, 42.

³² PCAOB Auditing Standard No. 2 ¶¶ 113, 115.

³³ PCAOB Auditing Standard No. 2 ¶¶ 40, 42, 178.

³⁴ PCAOB Auditing Standard No. 2 ¶ 40.

³⁵ PCAOB Auditing Standard No. 2 ¶ 24.

³⁶ PCAOB Auditing Standard No. 2 ¶ 140.

³⁷ PCAOB Auditing Standard No. 2 ¶ 26.

³⁸ PCAOB Auditing Standard No. 2 ¶ 24.

PCAOB auditing standards require the independent auditor to assess the “[a]dequacy of the internal audit activity and whether the internal audit function reports directly to the audit committee, as well as the extent of the audit committee’s involvement and interaction with internal audit. . . .”⁴¹ If this evaluation finds an internal audit function to be ineffective, the independent auditor must, at a minimum, issue a finding of a significant deficiency to the audit committee.⁴² An ineffective internal audit function, moreover, is a “strong indicator” of a material weakness.⁴³

PCAOB Chief Auditor Douglas Carmichael, in an interview with the Association of Certified Fraud Examiners to be published next month, described a “strong indicator” as shifting responsibility to substantiate that it is not a material weakness.⁴⁴ Companies with ineffective audit functions thus are likely to receive an adverse

opinion on the effectiveness of internal control over financial reporting.

Closing Thoughts

Prior to Sarbanes, compliance and finance personnel could, if they chose, have had little interaction. The post-Sarbanes environment requires an integrated approach, particularly in the fraud area, as fraud is both a compliance and controls issue.

The elements, whether they be judged under COSO or the FSG, must all work together to form an effective anti-fraud program. Companies that establish anti-fraud 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.

⁴¹ PCAOB Auditing Standard No. 2 ¶ 24.

⁴² PCAOB Auditing Standard No. 2 ¶ 140.

⁴³ PCAOB Auditing Standard No. 2 ¶ 140.

⁴⁴ D. Carozza, “*Giving SOX and Fraud Examiners Genuine Clout*,” The White Paper (May 2004).