7

Accounting, Internal Controls, and Audits

Enron was primarily an accounting scandal, little different from the 150-plus other accounting fraud cases that the SEC investigates in most years. Indeed, this was true not just of Enron, but also most of the other recent corporate scandals. Management relied upon the substantial flexibility inherent in GAAP to manage earnings and manipulate financial data so that operating results conformed to forecasts. The goal was to keep the firm's stock price high so that the managers could profit from their stock options. Because a standard accounting audit is not a true forensic audit designed to uncover wrongdoing, but rather only a sampling audit that may entirely miss the problem, and because at least some accountants chose to overlook problems, many managers thought they could get away with cooking the books.

Not surprisingly, much of Sarbanes-Oxley is concerned with auditing and accounting. Congress set out to reform the accounting industry by establishing the PCAOB as a new regulator with real teeth. Congress also sought to remake the relationship between auditor and corporate client so as to reduce the conflicts of interest inherent in that relationship. Finally, Congress sought to reshape the intrafirm accounting process,

by imposing new rules on the audit committee (see the previous chapter) and the firm's internal control systems.

The PCAOB

Prior to Sarbanes-Oxley, the accounting profession was largely self-regulating. The key actors—FASB and the AICPA—were private sector entities subject to minimal SEC oversight. FASB set accounting standards, while the AICPA provided guidance and contributed to the development of generally accepted principles and standards.

SOX shook up that cozy little world in a big way. Section 101 established the PCAOB as a nonprofit corporation to "oversee the audit of public companies that are subject to the securities laws." Funding for its operations comes from a special tax—called an accounting support fee—on public corporations. The fee varies with company size, specifically with the company's "average monthly U.S. equity market capitalization," so that larger firms bear a higher share of the burden.

The five members of the PCAOB's board must be "prominent individuals of integrity and reputation who have a demonstrated commitment to the interests of investors and the public," no more than two of whom can be CPAs. The SEC appoints the board members, in consultation with the chairman of the Federal Reserve Board and the secretary of the Treasury. The members serve five-year terms. The SEC can remove board members for good cause. The chairman of the board may not have been a practicing CPA within the five years prior to his or her appointment. While serving as a PCAOB board member, no one may receive payments from a public accounting firm other than fixed retirement income.

SOX § 101(c) specifies the PCAOB's duties, the most important of which are:

1. Develop a system for registration of public accounting firms that prepare audit reports for reporting companies. Per SOX § 102, only registered accounting firms can audit the books of reporting companies. In order to register, an accounting firm must make extensive disclosures about its clients, fees, and practices, as well as consent to cooperate in any PCAOB investigation.
2. Establish standards governing auditing, quality control, ethics, independence, and other matters relating to the preparation of audit reports for reporting companies.
3. Conduct regular inspections of registered public accounting firms to ensure that the firms are complying with PCAOB and SEC rules. Large accounting firms (with more than 100 reporting company clients) get inspected annually, while smaller ones are inspected every three years. If the PCAOB finds any violations, it reports them to the SEC and any relevant state accountant licensing board. Even if the PCAOB finds no violations, it still must send a written report to the SEC and the relevant state agencies.
4. Conduct investigations and disciplinary proceedings of misconduct by registered public accounting firms and any individuals associated with such firms. The PCAOB can impose a wide range of sanctions on violators, up to and including permanent revocation of the right to conduct audits of reporting companies.

   For more information about the PCAOB, visit their Web site: *www.pcaob.org/About_the_PCAOB/index.aspx.*

The Relationship Between the PCAOB and FASB

Sarbanes-Oxley § 103 gives the PCAOB what the Senate committee report on the act called "plenary authority" to set accounting standards. The PCAOB thus can adopt, amend,

or pre-empt guidance issued by the AICPA and other private sector groups. To date, except where SOX clearly requires otherwise, the PCAOB mostly has simply adopted the pre-existing standards set by the AICPA. In effect, however, the act downgrades the AICPA's role in the standard-setting process to merely advisory.

A mid-2004 change in how audit reports are drafted forcefully illustrated the PCAOB's new predominance in the standard-setting area. In the past, a reporting company's auditors would certify that the audit was conducted in accordance with GAAS and that the financial statements fairly and accurately represented the company's condition in accordance with GAAP. Since May 2004, however, the PCAOB requires audit reports to state that the audit and financial statements comply with "the standards of the Public Company Accounting Oversight Board."

The PCAOB doesn't have the field entirely to itself, however. SOX § 108 authorizes the SEC to "recognize, as 'generally accepted' for purposes of the securities laws, any accounting principles established by a standard setting body" that meets the following conditions:

- The body is a private entity.
- The body is governed by a board of trustees, the majority of whom are not, or have not been during the past two years, associated with any registered public accounting firm.
- The body "has adopted procedures to ensure prompt consideration, by majority vote of its members, of changes to accounting principles necessary to reflect emerging accounting issues and changing business practices" and "considers, in adopting accounting principles, the need to keep standards current in order to reflect changes in the business environment, the extent to which international

convergence on high quality accounting standards is necessary or appropriate in the public interest and for the protection of investors."

- The SEC determines that the body has the capacity to assist the commission in carrying out its duties "because, at a minimum, the standard setting body is capable of improving the accuracy and effectiveness of financial reporting and the protection of investors under the securities laws."

In April 2003, the SEC recognized FASB as such a standard-setting body. Accordingly, FASB now receives funding from the same user fees that support the PCAOB. In addition, FASB functions as a separate standard setter working in parallel with the PCAOB.

The relationships between the SEC, PCAOB, FASB, and AICPA are fraught with the potential for conflict. To date, the three private sector entities have managed to work together in a reasonably cooperative manner. In general, the PCAOB has primary responsibility for GAAS, the FASB for GAAP, and the AICPA for nonreporting company accounting rules, but there seems to be a good deal of mutual consultation. In the event of conflict, of course, the SEC's oversight role gives it the last word.

The PCAOB and State Licensing

Like lawyers, physicians, dentists, and various other professionals, accountants traditionally are licensed for practice by states rather than the federal government. The PCAOB does not displace this system of state licensing and regulation. Instead, the two work in tandem. A CPA thus must be licensed by the state to practice accounting; if the CPA's practice includes auditing the books of reporting companies, the CPA's accounting firm also must be registered with the PCAOB.

PCAOB standards governing auditing of reporting companies will pre-empt any contrary state regulations, but this leaves the states as the primary regulator for audits of nonreporting companies. In general, of course, states simply mandate compliance with GAAS and GAAP.

There's clearly a need for effective coordination between the PCAOB and state licensing bodies, both so that accounting practices and auditing standards remain reasonably uniform across all types of companies and so that individuals or firms disciplined at one level are also investigated at the other. Here, again, is a role for the SEC to use its oversight authority to encourage such cooperation.

New Rules for the Auditor-Client Relationship

At Enron and other firms, the audit process broke down in part because accountants got too cozy with their clients. Sarbanes-Oxley included a number of provisions designed to put some space back between client and outside auditor.

Limits on Nonaudit Services

As we saw in Chapter 1's review of the business failures of 2000–2002, a key concern motivating SOX's drafters was the conflict of interest inherent when accounting firms sell other services to the corporations whose books they audit. Title II of the act therefore limited the extent to which accountants may provide consulting services to their audit clients. Some nonaudit services were banned outright. The outside auditor, for example, may not provide bookkeeping or related services, design or implement financial information systems, provide fairness opinions in connection with corporate transactions, conduct internal audits on an outsourced basis, provide humans relations services, or act as an investment banker

or legal expert. In addition, the PCAOB is authorized to ban other nonaudit services as it deems fit.

Did Providing Nonaudit Services Really Compromise Auditor Independence?

Yale law professor Roberta Romano compiled the results of numerous studies of auditor performance and concluded that the "overwhelming majority" "suggest that SOX's prohibition of the purchase of non-audit services from an auditor is an exercise in legislating away a non-problem." Most of the studies found that there was no connection between provision of nonaudit services and the quality of the audit. Several even found that auditors who provided nonaudit services performed higher quality audits, presumably because providing such services gives the auditor more and better information about the company. You can read her analysis at *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=596101*.

Contrary to conventional wisdom, however, SOX did not completely ban all such services. Provided the client's audit committee approves the retention in advance, in fact, the auditor may perform any nonaudit services not banned by SOX or the PCAOB. For example, a corporation's outside auditor can also prepare its corporate tax returns. It's advisable, however, to check with legal counsel before asking the auditor to perform any nonaudit services.

The SEC requires disclosure of any "fees paid to the independent accountant for (1) audit services, (2) audit-related services, (3) tax services, and (4) other services" in the annual

report on Form 10-K. The SEC has also cautioned companies that there are "some circumstances where providing certain tax services to an audit client would impair the independence of an accountant, such as representing an audit client in tax court or other situations involving public advocacy."

The SEC did create an exception for *de minimis* nonaudit services, pursuant to which a registered accounting firm still is independent even if it provides nonapproved, nonaudit services. The aggregate compensation for all such services may constitute no more than 5 percent of the total fees paid the auditor by the client during the relevant fiscal year. Once the company recognizes that it is compensating its auditor for nonaudit services without prior approval by the audit committee, the management promptly must bring the oversight to the audit committee's attention and have the services approved by the committee.

Auditors Work for the Audit Committee

As we saw in Chapter 6, SOX significantly expanded the role of the audit committee of the board of directors. Many of these new rules directly affect the reporting company's outside auditor. It is now the audit committee, for example, that must select the reporting company's outside auditor and negotiate the auditor's fees. The audit committee must approve (typically in advance) any nonbanned, nonaudit services the auditor provides to the corporation.

SOX clarified that the outside auditor is responsible to the audit committee, rather than management. The outside auditors must periodically meet with the audit committee outside the presence of management. At least annually, the outside auditor of a NYSE-listed company must give the audit committee a report detailing: (1) the firm's internal control procedures; (2) any material problems identified in the most recent

internal control review, or by any government or other regulatory body investigation; (3) any steps taken to deal with any such problems; and (4) all relationships between the independent auditor and the listed company. Obtaining such a report has become best practice for non-NYSE firms, as well.

The auditor should report to the audit committee any disagreement between management and the auditor as to financial reporting. If the disagreement is resolved, the auditor still must report it to the audit committee, and also report on the manner in which it was dealt with. If a dispute is not resolved between management and the auditor, it is up to the audit committee to solve the problem.

Where GAAP provides options as to how to disclose information, the auditor should flag the issue for the audit committee. The auditor should discuss the alternatives with the audit committee and identify the disclosure it preferred.

No Coercing the Auditor

SOX § 303 makes it unlawful for an officer or director of a reporting company, or anyone acting under their orders, to "fraudulently influence, coerce, manipulate, or mislead any independent" CPA "engaged in the performance of an audit" of the company's financial statements "for the purpose of rendering such financial statements materially misleading." The SEC defines *officer* for this purpose as including "the company's 'president, vice president, secretary, treasurer or principal financial officer, comptroller or principal accounting officer, and any person routinely performing corresponding functions.'"

Per the SEC rules implementing § 303, the prohibition doesn't apply just to employees of the reporting company acting under orders from directors or officers of the company:

> In other words, someone may be "acting under the direction" of an officer or director even if they are not under the supervision or control of that officer or director. Such persons might include not only the issuer's employees but also, for example, customers, vendors or creditors who, under the direction of an officer or director, provide false or misleading confirmations or other false or misleading information to auditors, or who enter into "side agreements" that enable the issuer to mislead the auditor. In appropriate circumstances, persons acting under the direction of officers and directors also may include not only lower level employees of the issuer but also other partners or employees of the accounting firm (such as consultants or forensic accounting specialists retained by counsel for the issuer) and attorneys, securities professionals, or other advisors who, for example, pressure an auditor to limit the scope of the audit, to issue an unqualified report on the financial statements when such a report would be unwarranted, to not object to an inappropriate accounting treatment, or not to withdraw an issued audit report on the issuer's financial statements.

The SEC likewise has provided guidance as to the kinds of conduct deemed improper influence:

- Offering or paying bribes or other financial incentives, including offering future employment or contracts for nonaudit services
- Providing an auditor with an inaccurate or misleading legal analysis
- Threatening to cancel or canceling existing nonaudit or audit engagements if the auditor objects to the issuer's accounting

- Seeking to have a partner removed from the audit engagement because the partner objects to the issuer's accounting
- Blackmailing or making physical threats

This list is not exclusive and under appropriate circumstances other conduct could be a violation. Among other potentially prohibited conduct is "knowingly providing to the auditor inadequate or misleading information that is key to the audit, transferring managers or principals from the audit engagement, and when predicated by an intent to defraud, verbal abuse, creating undue time pressure on the auditors, not providing information to auditors on a timely basis, and not being available to discuss matters with auditors on a timely basis."

Miscellaneous Rules

Congress considered requiring reporting companies to rotate their outside auditor periodically, but ultimately decided not to go that route. Instead, SOX § 203 requires registered public accounting firms to rotate (1) the partner having primary responsibility for the audit and (2) the partner responsible for reviewing the audit every five years. The audit committee must ensure that the requisite rotation actually takes place.

As a matter of good practice, a company ought to consider rotating audit firms periodically so as to get the benefit of a fresh set of eyes. Some corporate governance experts recommend doing so at least every ten years. In addition, governance experts recommend rotating audit firms if a substantial number of former company employees have gone to work for the audit firm or vice-versa.

A separate rule imposes a cooling-off period, pursuant to which an employee of a registered accounting firm may not go

to work for a client on whose audit team the employee served until one year after ceasing to be a member of the audit team.

The registered accounting firm may not compensate an audit partner based on the amount of nonaudit services the client purchases.

The auditor and its employees may not have any financial interest in the client or any business relationship with the client excepting, of course, the audit relationship and any authorized nonaudit services.

Finally, SOX requires that registered accounting firms retain records relating to audits of reporting companies for at least seven years. The prohibition applies to both shredding of physical documents and purging of electronic records. It also applies to all work papers and other interim documentation, as well as final reports.

General Standards of Auditor Independence

In addition to the specific rules we've been reviewing in this section, the SEC set up a backstop—a general expectation of auditor independence. According to the SEC, an auditor's independence is impaired either when the accountant is not in fact independent or when a reasonable investor would conclude, in light of the relevant facts and circumstances, that the auditor would not be capable of acting independently. Hence, any mutual or conflicting interest with the audit client would impair the auditor's independence. In addition, an independent auditor must recognize its obligations not only to management and the shareholders, but also to creditors and other corporate constituencies that rely on the objectivity of the company's financial statements.

Section 404: Internal Controls

For the board of directors and top management of a public corporation to discharge their obligations to oversee the financial reporting process, they must identify, understand, and assess the factors that may cause the financial statements to be fraudulently misstated. Sarbanes-Oxley § 404 creates an obligation to do so having real teeth:

> § 404. Management Assessment of Internal Controls
>
> (a) Rules Required.—The Commission shall prescribe rules requiring each annual report . . . to contain an internal control report, which shall—
>
> (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and
>
> (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.
>
> (b) Internal Control Evaluation and Reporting.—With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

If you parse that text, § 404 looks at first like a mere disclosure requirement. It requires inclusion of internal control disclosures in each public corporation's annual report. This disclosure statement must include: (1) a written confirmation by which firm

management acknowledges its responsibility for establishing and maintaining a system of internal controls and procedures for financial reporting; (2) an assessment, as of the end of the most recent fiscal year, of the effectiveness of the firm's internal controls; and (3) a written attestation by the firm's outside auditor confirming the adequacy and accuracy of those controls and procedures. It's not the disclosure itself that makes § 404 a headache, of course; instead, the problem is the need to assess and test the company's internal controls in order to be able to make the required disclosures.

Make no mistake; § 404 really is a headache. Study after study confirms that Section 404 has imposed huge costs on American business. According to a 2003 article in *USA Today*, for example, the CEOs of Affiliated Computer Services and Steelcase both said that their companies will spend 20,000 staff hours to comply with § 404, which is the equivalent of ten people working full-time for a year! (When SOX was under consideration, the SEC estimated only 383 staff hours would be required, which has proven to be one of the more laughable underestimates in recent memory.) A survey by Foley & Lardner found that the average cost of being public for a company with annual revenue under $1 billion increased by $1.6 million—130 percent—after SOX went into force. And because a lot of SOX § 404 compliance costs are fixed—that is, they don't depend on firm size—the cost of complying weighs especially heavily on smaller firms (see Chapter 1, page 5).

Internal Controls Defined

During the Congressional hearings that led up to Sarbanes-Oxley, internal controls generated most of the buzz. Enron, WorldCom, and most of the world's other ills were blamed on failed internal controls. Not surprisingly, they got a lot of attention from Congress.

Unfortunately, the phrase *internal controls* has a long and contested meaning in the accounting profession. Worse yet, Congress compounded the problem by using the phrase in two different sections of SOX with very different meanings.

As we saw in Chapter 3, SOX § 302 requires a reporting company's CEO and CFO to certify, among other things, that the company has "internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities." In a June 2003 statement, the SEC explained that internal controls as used in § 302 therefore refers to "disclosure controls and procedures," which the SEC in turn defined "to mean controls and procedures of a company that are designed to ensure that information required to be disclosed by the company in the reports that it files or submits under the Exchange Act is recorded, processed, summarized and reported, within the time periods specified in the Commission's rules and forms." In other words, for purposes of a § 302 certification, the question is whether the company has established appropriate procedures to ensure that the information contained in documents like the 10-K and 10-Q reports is accurate and complete.

In contrast, § 404 refers to "internal control structure and procedures for financial reporting." According to the SEC, the set of internal controls to which § 404 refers is narrower than those dealt with under § 302. Specifically, the SEC defines "internal control" for purposes of § 404 as:

> A process designed by, or under the supervision of, the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes

in accordance with generally accepted accounting principles and includes those policies and procedures that

- pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the registrant;
- provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and receipts and expenditures of the registrant are being made only in accordance with authorizations of management and directors of the registrant; and
- provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on the financial statements.

In other words, the term *internal controls* as used in § 404 refers to the processes the company uses to ensure that its financial statements comply with GAAP and are free from material misrepresentations and omissions.

Basic Principles for Assessing Internal Controls

According to the SEC guidance proposed in December 2006, management's assessment per § 404 is to be guided by two basic principles. First, management should evaluate the company's existing internal controls over financial reporting to determine whether there is a reasonable possibility that those controls would not prevent or detect a material misstatement in the financial statements. Management need not assess all of the various internal controls or other law compliance programs the company may have implemented, but rather should focus on those controls intended or necessary to prevent or detect

such a material misstatement. In adopting this principle, the SEC stressed that a considerable portion of the unexpectedly high costs of complying with § 404 are attributable to excessive testing of controls.

Second, management's assessment of the design and operation of the company's internal controls over financial reporting should be risk based. Put another way, management focuses its evaluation on those areas of financial reporting that pose the greatest risks of material errors in the company's financial disclosures.

To assist companies in implementing these principles, the SEC identifies four basic components of the § 404 compliance process. First, management should identify the principal risks to accurate financial disclosures posed by its business and the existing controls, if any, designed to address those risks. As such, the SEC's guidance reflects the principle of a risk-based approach to internal controls. Implementing that principle requires management to exercise judgment in separating those areas of its accounting and financial reporting operations that are both material and by their nature present a risk of intentional or negligent errors in financial reporting. The SEC explains that "financial reporting elements would generally have higher risk when they include transactions, account balances or other supporting information that is prone to misstatement. For example, elements which: (1) involve judgment in determining the recorded amounts; (2) are susceptible to fraud; (3) have complexity in the underlying accounting requirements; or (4) are subject to environmental factors, such as technological and/or economic developments, would generally be assessed as higher risk." The SEC calls particular attention to those areas "involving significant accounting estimates, related party transactions, or critical accounting policies," which generally should be assessed as having "higher risk for both the risk

of material misstatement to the financial reporting element and the risk of control failure." Having identified the areas of high risk, management then must identify the existing controls designed to reduce the risk of a material misstatement in these areas. Only those controls must be included in management's § 404 assessment report.

Second, once management has identified the controls that must be assessed, management then gathers and analyzes evidence as to whether those controls are effective in preventing or timely detecting financial reporting fraud or errors. Although management's § 404 assessment report is based on whether any material weaknesses exist as of the end of the fiscal year, the SEC's guidance encourages management to exercise informed judgment in adapting its existing daily business, self-assessment, and other monitoring activities to provide the basis for its § 404 assessment report. According to the SEC, tying the § 404 assessment to existing compliance activities will reduce costs by obviating the need for an annual internal § 404 audit.

Third, based on the evidence it gathers in the second phase, management must determine whether there are any deficiencies in its internal controls. If so, management must decide whether the identified deficiencies are material weaknesses. For this purpose, the SEC defines a material weakness as "a deficiency, or combination of deficiencies, in ICFR such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis by the company's ICFR." If a deficiency rises to the level of a material weakness, management's assessment report must state that the company's internal controls over financial reporting are not effective.

Finally, management must document the processes by which its assessment report was prepared and the evidence it gathered

and evaluated in the course of its assessment. The SEC encourages management to exercise informed judgment in deciding the form the documentation will take. In practice, as discussed below, most companies rely on the emerging suites of § 404 compliance software tools to provide the requisite documentation.

Selecting a Framework for Conducting the § 404 Assessment

The SEC rules implementing § 404 require that all reporting company managers base their assessment on "a suitable, recognized control framework." The only framework for conducting the assessment to date approved by the SEC is the Internal Control–Integrated Framework (ICIF), which was promulgated by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Unfortunately, while the COSO framework sets out the elements of an effective internal control system, it provides very limited directions on how actually to go about evaluating the company's internal controls over financial reporting.

The COSO framework sets out three broad areas in which companies should have systems of internal control: the reliability of the company's financial reporting, the effectiveness and efficiency of company operations, and the company's compliance with applicable laws and regulations. Section 404 and the SEC rules thereunder, of course, only mandate corporate compliance with the first area.

The COSO framework evaluates company performance with respect to each of the base objectives using five components: risk assessment, control environment, control activities, information and communication, and monitoring. COSO further broke down these components to set out twenty basic principles:

Control Environment

1. Integrity and Ethical Values. Sound integrity and ethical values, particularly of top management, are developed and understood and set the standard of conduct for financial reporting.
2. Board of Directors. The board of directors understands and exercises oversight responsibility related to financial reporting and related internal control.
3. Management's Philosophy and Operating Style. Management's philosophy and operating style support achieving effective ICFR [i.e., internal controls for financial reporting].
4. Organizational Structure. The company's organizational structure supports effective ICFR.
5. Financial Reporting Competencies. The company retains individuals competent in financial reporting and related oversight roles.
6. Authority and Responsibility. Management and employees are assigned appropriate levels of authority and responsibility to facilitate effective ICFR.
7. Human Resources. Human resource policies and practices are designed and implemented to facilitate effective ICFR.

Risk Assessment

8. Financial Reporting Objectives. Management specifies financial reporting objectives with sufficient clarity and criteria to enable the identification of risks to reliable financial reporting.
9. Financial Reporting Risks. The company identifies and analyzes risks to the achievement of financial reporting

objectives as a basis for determining how the risks should be managed.

10. Fraud Risk. The potential for material misstatement due to fraud is explicitly considered in assessing risks to the achievement of financial reporting objectives.

Activities

11. Integration with Risk Assessment. Actions are taken to address risks to the achievement of financial reporting objectives.
12. Selection and Development of Control Activities. Control activities are selected and developed considering their cost and their potential effectiveness in mitigating risks to the achievement of financial reporting objectives.
13. Policies and Procedures. Policies related to reliable financial reporting are established and communicated throughout the company, with corresponding procedures resulting in management directives being carried out.
14. Information Technology. Information technology controls, where applicable, are designed and implemented to support the achievement of financial reporting objectives.

Information and Communication

15. Financial Reporting Information. Pertinent information is identified, captured, used at all levels of the company, and distributed in a form and timeframe that supports the achievement of financial reporting objectives.
16. Internal Control Information. Information used to execute other control components is identified, captured, and distributed in a form and timeframe that

enables personnel to carry out their internal control responsibilities.

17. Internal Communication. Communications enable and support understanding and execution of internal control objectives, processes, and individual responsibilities at all levels of the organization.
18. External Communication. Matters affecting the achievement of financial reporting objectives are communicated with outside parties.

Monitoring

19. Ongoing and Separate Evaluations. Ongoing and/or separate evaluations enable management to determine whether ICFR is present and functioning.
20. Reporting Deficiencies. Internal control deficiencies are identified and communicated in a timely manner to those parties responsible for taking corrective action, and to management and the board as appropriate.

In order to operationalize the generalities of the COSO framework, most reporting companies have looked to PCAOB Auditing Standard No. 2, which sets out the standards by which PCAOB-registered auditors are to conduct "An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements." Although Audit Standard No. 2 is intended for use by, and solely binding on, auditors, according to the SEC "many companies indicated that the scope of their management's evaluation process and the methods and procedures used for testing controls were modeled after its requirements."

PCAOB Auditing Standard No. 2 is available at *www.pcaobus.org/Standards/Standards_and_Related_Rules/Auditing_*

Standard_No.2.aspx. The PCAOB also makes an extensive set of questions and answers about Auditing Standard No. 2 available online at *www.pcaob.org/Standards/Staff_Questions_and_Answers/index.aspx.*

In addition to providing a framework for conducting the assessment mandated by § 404, PCAOB Auditing Standard No. 2 also imposes four specific responsibilities on company management:

a. Accept responsibility for the effectiveness of the company's internal control over financial reporting;
b. Evaluate the effectiveness of the company's internal control over financial reporting using suitable control criteria;
c. Support its evaluation with sufficient evidence, including documentation; and
d. Present a written assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year.

COSO AND AS 2 ONLINE

An executive summary of COSO's statement "Internal Control over Financial Reporting—Guidance for Small Public Companies" is available at *www.coso.org/Publications/SB_Executive_Summary.pdf.*

Failure by management to satisfy those obligations will result in adverse opinion by the auditor.

As this book goes to press, the PCAOB is developing a new auditing standard that would:

Direct the auditor to the most important controls and emphasize the importance of risk assessment;

- Revise the definitions of significant deficiency and material weakness, as well as the "strong indicators" of a material weakness;
- Clarify the role of materiality, including interim materiality, in the audit;
- Remove the requirement to evaluate management's process;
- Permit consideration of knowledge obtained during previous audits;
- Direct the auditor to tailor the audit to reflect the attributes of smaller and less complex companies;
- Refocus the multi-location testing requirements on risk rather than coverage; and
- Recalibrate the walkthrough requirement.

As with the SEC guidance issued at roughly the same time, the goal is to reduce compliance costs by focusing Section 404 audits on those areas most likely to result in material misstatements or omissions in the company's financial statements. Because auditors still must annually opine on the effectiveness of their client's internal controls, the extent to which the SEC guidance and PCAOB actions will actually reduce costs will depend in large part how auditors interpret the new standard.

The text of the new auditing standard, as proposed, is available at *www.pcaobus.org/Rules/Docket_021/2006-12-19_Release_No._2006-007.pdf.*

An Overview of § 404 Compliance from Management's Perspective

Section 404 imposes duties on both the management and outside auditor of a reporting company. As the PCAOB explains:

> The auditor's report on internal control over financial reporting does not relieve management of its responsibility for assuring users of its financial reports about the effectiveness of internal control over financial reporting.

In this section, we'll take a walk through the § 404 process from management's perspective.

The Audit Committee's Role

Although § 404 refers to management's responsibility, the audit committee should be an active player in § 404 compliance. KPMG partner Kenneth Daly, in an article for *Risk Management* magazine, recommends that "the audit committee must understand where the company is in the process, as well as the critical elements of the plan that will move the company's compliance program forward. The audit committee should monitor management's progress and ask key questions to help evaluate the state of the section 404 compliance process. It is important to ensure that the right questions are directed to the appropriate management personnel. For example, if the audit committee wants to know whether internal audit's resources are adequate, it should ask the director of internal audit, as well as the CFO. Posing the same question to different levels of management and to different managers also may reveal areas of the compliance process that require attention. Questions that audit committees might ask should revolve around process optimization, technology, organization and people, and risk and control."

Whole books have been written on § 404. PCAOB Auditing Standard No. 2 itself weighs in at 220-plus pages, not counting another 150-plus pages of appendixes. In addition, as the SEC stressed, the process necessarily varies from company to company. Accordingly, this section provides a very general overview. Companies preparing to comply with their obligations under § 404 need to consult with legal counsel and their outside auditor before beginning the process.

At the outset, managers responsible for § 404 compliance must recognize that this is a process rather than a project. Although the first year a company must comply with § 404 likely will be the most costly and time consuming, as well as offering the greatest risk of an adverse auditor opinion, both the management assessment and auditor attestation must be performed every year. It's for this reason, of course, that § 404 costs are a recurring item.

One way in which the SEC's 2006 guidance may prove helpful in cost-containment, however, is by reminding management that, while the Section 404 assessment must be undertaken annually, "subsequent evaluations should be more focused on changes in risks and controls rather than identification of all financial reporting risks and the related controls. Further, in each subsequent year, the evidence necessary to reasonably support the assessment will only need to be updated from the prior year(s), not recreated anew." In implementing this guidance, firms should develop processes for creating an institutional memory so that changes in personnel at either the firm or its auditor do not require reinventing the wheel.

Both the PCAOB and SEC emphasize that § 404 requires a top-down approach, a point that was strongly re-emphasized in the 2006 guidance they provided. The § 404 team therefore starts with controls that apply company-wide. The team

then evaluates controls that apply to particular business units or functions. Next, the team looks at how particular business units handle significant accounts. Finally, the team evaluates how transactions in those accounts are processed.

Putting Together a § 404 Team

HP published a white paper summarizing how it went about complying with § 404. Candidly, the paper is mostly a sales brochure for HP software, but it does have some useful information. For example, we learn that HP set up "a core team consisting of seven professionals who had direct responsibility" for HP's § 404 compliance process. The team leader came from HP's controller's office and included representatives from "Internal Audit, Application Development, Managed Services, and some of the business units." This sort of cross-function, multidisciplinary team is an emerging best practice. Ideally, the team should have some continuity of membership from year-to-year to both hold down costs and develop institutional memory.

Likewise, both the SEC and PCAOB insist that companies should devote most attention to those high-risk areas most likely to result in financial reporting problems, which supposedly allows management to contain costs by focusing on those controls and areas where there is a particular risk of a material misstatement occurring in the company's financial statements. To take a basic example, a COSO study found that over 50 percent of financial fraud involved overstating revenues either by recognizing revenue prematurely or by booking fictitious revenue. A company therefore would be foolish not

to devote considerable attention to the internal controls it uses to monitor revenue recognition. Accordingly, we'll use revenue recognition as an example of how the internal control audit might work.

At the company-wide control level, controls for revenue recognition would start with distribution of written policy manuals setting out the rules by which the company recognizes revenue and the procedures for doing so. In addition, the company should mandate regular training of both sales and accounting personnel.

Documentation is an essential part of the internal control assessment. Accordingly, not only copies of the policy manual, but also records of attendance at training sessions should be maintained. There's a growing array of software packages available designed to assist with § 404 compliance, most of which include some sort of database system for maintaining electronic copies of the requisite documentation.

Other High Risk Areas

In addition to revenue recognition, four other areas have proven especially common sources of financial fraud: (1) stock options and other issuance of equity securities, (2) accounting for reserves, accruals, and contingencies, (3) capitalization of expenses, and (4) inventory levels. All of these are areas where attention should be devoted during the § 404 assessment process.

Moving down the ladder from the company-wide to the business-unit level, one next would look at large, one-time, or otherwise unique contracts that account for a material share of

the company's revenues. An adequate system of internal control requires that the company's internal auditors review the terms of the contract to determine when and how revenues from it should be recognized. In addition, internal audit should double-check the work of the business unit, by confirming the details of the contract with the other party.

Internal Auditors

NYSE-listed companies are required to have an "internal audit function to provide management and the audit committee with ongoing assessments of the company's risk management processes and system of internal control." The company may outsource this function, although not to the company's outside auditor. Among non-NYSE companies, having an internal auditor is becoming a recognized best practice.

The Institute of Internal Auditors, a trade association, explains that: "Although they are independent of the activities they audit, internal auditors are integral to the organization and provide ongoing monitoring and assessment of all activities. On the contrary, external auditors are independent of the organization, and provide an annual opinion on the financial statements." In other words, internal auditors work for management (and the audit committee). At many companies, they play a key role in § 404 compliance.

Note that the SEC's rules on the independence of outside auditors forbid the outside auditor from designing or testing a company's internal controls. This is an important reason for companies to have an internal audit unit.

The next step down will involve looking at how the company handles routine transactions. Suppose you're on the § 404 compliance team at Acme, a manufacturing company. Like most companies, Acme provides quarterly revenue forecasts for stock market analysts. Acme's top management puts a lot of pressure on employees to "make the number." Suppose Acme is basically healthy, but internal projections suggest that it may not meet its earnings forecasts for the first quarter of the year. Quarterly revenue numbers could be tweaked to help the company meet its earnings forecast in a variety of ways. Acme could backdate shipping records, for example, so that revenue for products actually shipped in the second quarter is recognized in the first quarter. Alternatively, products returned in the first quarter might not be booked until the second quarter, so as to delay the resulting hit to earnings. In the worst case, Acme management might actually report fictitious revenue by claiming to have shipped products that never existed.

There are lots of other ways for creative managers under pressure to cook the revenue books. In 2003, for example, the SEC charged that Internet real estate company Homestore artificially inflated revenues through so-called roundtrip deals:

> In these round-trip transactions, Homestore paid inflated sums to various vendors for services or products, and, in turn, the vendors used these funds to buy advertising from two media companies. The media companies then bought advertising from Homestore, and Homestore improperly recorded the money it received from the sale of such advertising as revenue in its financial statements. The essence of these transactions was a circular flow of money by which Homestore recognized its own cash as revenue.

An effective system of internal controls will include procedures for ensuring that the responsible personnel treat these sort of routine transactions properly from an accounting perspective. One important control is a walkthrough, by which the internal auditors (or their equivalent) observe how a sample transaction is processed. In a manufacturing company, there should be mechanisms in place for internal audit to meet with the personnel in charge of shipping and receiving to check on shipments and returns, dating of shipping and return documents, and the like. Similarly, internal audit should check inventory levels.

More on Revenue Recognition

Revenuerecognition.com offers a wide range of resources dealing with revenue recognition tailored for financial executives.

Internal controls must be effective as to both their design and operation. Accountant Jack Paul, in an online article for *The CPA Journal*, explains the difference between the two as follows:

> Whereas design effectiveness pertains to whether a control is properly crafted, operating effectiveness deals with use of a properly designed control to prevent, detect, or correct misstatements or irregularities on a timely basis. For example, a daily reconciliation of cash receipts is not effectively designed when the cashier performs the reconciliation. But if an independent person is designated to perform the reconciliation and the other procedures are properly documented, the control is effectively designed. The

> control is not operating effectively when the independent reconciler either fails to perform the reconciliation daily or does so in a perfunctory manner. Design effectiveness of this control could be tested by reviewing documentation to ensure that the procedures are satisfactory. Operating effectiveness could be tested by examining the reconciler's initials on the daily reconciliation sheet.

Internal controls can also be divided between those relating to how transactions flow within a company and those that deal with static data, such as account balances. Again, Jack Paul explains:

> Examples of controls relating to transaction flows include approving cash disbursements; prelisting cash receipts; approving credit sales; and matching purchase orders, vendor invoices, and receiving reports when booking accounts payable. Controls over balances (stocks) include periodic reconciliation of bank accounts; reconciliation of subsidiary ledgers with control accounts; procedures for physical inventory counts; and controls governing the periodic preparation of financial statements. Overarching controls include the factors comprising the control environment. Overarching controls and those pertaining to flows operate continuously throughout the fiscal period; controls relating to balances typically operate less frequently. Thus bank accounts are reconciled monthly, whereas controls over cash flows are continuous.

The annual management assessment confirms and documents that these sorts of controls exist and are functioning properly. Increasingly, companies rely on comprehensive software packages both to document and test their internal controls. Many of these packages integrate § 404 compliance with the § 302 certification process, so as to help contain costs.

Using a single software platform/electronic repository to coordinate and document all controls, documentation, test results, and other relevant supporting materials is useful for several reasons. First, it reduces audit fees. You can simply point your outside auditor at a single repository rather than requiring the auditor to check multiple programs across multiple departments. Second, it ensures adequate documentation in case the SEC challenges the company's compliance. Third, it helps ensure that the company retains key financial reporting documents in accordance with SOX's document retention rules. Finally, a common software platform can provide a central enterprise-wide set of controls. The WorldCom scandal nicely illustrates the potential problems that can arise if your company lacks such controls. As described by a federal court:

> A contributing factor that allowed the books to be deliberately falsified without attracting much notice was that the Company's internal controls over the preparation and publication of its financial results were dysfunctional at best, and in some areas controls were missing entirely. WorldCom's accounting systems had not kept pace with the growth in the Company due to its feverish pace of acquisitions and management neglect. Numerous legacy financial systems were being operated by different WorldCom units, and producing consolidated financial statements required patchwork software and significant manual processing. (*S.E.C. v. Worldcom, Inc.*, 2003 WL 22004827 [S.D.N.Y., Aug 26, 2003]).

Indeed, it's partly to prevent such breakdowns that the SEC and PCAOB insist on a top-down approach to § 404 compliance.

1. Lack of an enterprise-wide, executive-driven internal control management program.
2. Lack of a formal enterprise risk management program.

3. Inadequate controls associated with the recording of nonroutine, complex, and unusual transactions.
4. Ineffectively controlled post-merger integration.
5. Lack of effective controls over the IT environment.
6. Ineffective financial reporting and disclosure preparation processes.
7. Lack of formal controls over the financial closing process.
8. Lack of current, consistent, complete, and documented accounting policies and procedures.
9. Inability to evaluate and test controls over outsourced processes.
10. Inadequate board and audit committee understanding of risk and control.

Ten Top Material Weaknesses

Albert Lilienfeld of Deloitte & Touche LLP, in an article from the collection *Audit Committee Workshop 2005* (a publication of the Practicing Law Institute), offers the above top ten list of potential material weaknesses to which management and auditors should pay particular attention.

Under SEC rules, management cannot claim that its internal controls are effective if one or more material weaknesses exist. In addition, the existence of any material weakness and the steps being taken to correct it must be disclosed in the annual report on Form 10-K. For this purpose, a material weakness is defined by PCAOB Auditing Standard No. 2 as a "significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material

misstatement of the annual or interim financial statements will not be prevented or detected." In turn, significant deficiency is defined as a problem with the company's internal controls that "adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with generally accepted accounting principles such that 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." Internal controls do not have to operate perfectly to be considered effective, so long as the problems do not give rise to "more than a remote likelihood" that the company's financial reporting will be materially and adversely affected.

Significant deficiencies do not have to be disclosed, but as a matter of best practice should be addressed. If fixing a significant deficiency requires a material change to either the disclosure procedures certified per § 302 or to the § 404 internal controls over financial reporting, however, those changes must be disclosed. In that event, the significant deficiency motivating the change also should be disclosed.

The Auditor's Opinions

As implemented by PCAOB Auditing Standard No. 2, § 404 requires the reporting company's registered outside auditing firm to issue two opinions: (1) whether management's assessment of the company's internal controls fairly states the condition and effectiveness of those controls and (2) whether the auditor believes that the company has established effective internal controls over financial reporting.

In order for the auditor to issue an unqualified opinion that the company has the requisite effective controls, the auditor must find no material weaknesses in those controls. In contrast,

an auditor can issue an unqualified opinion as to management's assessment even if there are material weaknesses, so long as management's assessment disclosed those weaknesses. Recall that the auditor must issue a disclaimer (i.e., decline to express an opinion) if management fails to carry out its responsibilities under § 404 and/or limits the scope of the audit.

Definitional Changes

As this book went to press, the PCAOB planned three important amendments to the definitions of *significant deficiencies* and *material weaknesses*. First, in both definitions, the term "more than remote likelihood" would be replaced with the term "reasonable possibility." The goal here is to raise the threshold with respect to the likelihood of an occurrence and thus make clear that the mere risk of a misstatement is not enough to violate the standard. Second, in the definition of *material weakness,* the term "a significant deficiency, or combination of significant deficiencies" will be replaced with the term "a control deficiency, or combination of control deficiencies"; the goal is to make clear that auditors are not required "to search for deficiencies that, individually or in combination, are less severe than material weaknesses." Finally, in the definition of *significant deficiency,* the term "more than inconsequential" will be replaced with the term "significant." The goal here is to prevent auditors from spending "excess time identifying, discussing and fixing deficiencies that are not sufficiently important to the company's overall system of internal control."

The SEC and the PCAOB have emphasized that auditors should integrate their audit of the company's internal controls with their audit of the financial statements, so as to hold down the costs of complying with § 404.

In addition, the PCAOB's proposed amendments to Auditing Standard No. 2 would provide additional cost savings by eliminating the requirement that the auditor conduct an evaluation of management's assessment. As a result, if the proposal is adopted, it will eliminate "the separate opinion on management's assessment because it is redundant of the opinion on internal control itself and because the latter opinion more clearly conveys the same information—specifically, whether the company's internal control is effective."