CHAPTER 1

Introduction and Company Requirements

Chapter Summary

Consider the lessons learned since 2003 regarding the assessment and reporting on the effectiveness of internal control over financial reporting.

Gain an overview of the SEC rules requiring management's assessment of the effectiveness of the entity's internal control over financial reporting with commentary on the implications of these requirements.

Summarize ways that management can work with its auditors to create an efficient internal controls audit.

Lessons Learned

An advantage today of studying the requirements in the Sarbanes-Oxley Act of 2002 (SOX) that relate to reporting on internal controls over financial reporting is that some experience has been gained in performing this task and we have had a chance to watch larger, well-controlled companies struggle with the ambiguity of rules and regulations that were enacted in an environment of crisis. In response to that struggle, additional and clarified regulations were enacted to reduce the costs associated with compliance.

A genesis for the requirements can be seen in long-standing research findings that behind every previous cycle of company fraudulent activity, business failures, and alleged audit failures has been an underlying cause: weaknesses in internal control. What seems clear from the Enron, Worldcom, and other business disasters of the period just before the SOX legislation is that in the absence of structure and controls, the then-present regulatory and auditing requirements were insufficient to deter or prevent tinkering with

accounting results in such a way as to produce materially misstated financial statements.

No one is faulting management for being optimistic, nor auditors for trying to perform efficient audits, but when the combination of those objectives becomes a threat to the confidence in the U.S. securities market, something needs to be done. In addition to the company frauds that were revealed in the early-2000 period, there had been a steadily rising number of financial statement restatements in the 1990s and the trend was also becoming worrisome in terms of the reliability of financial reporting.

Was the underlying cause of the restatement mess the lack of attention to accounting detail by company accounting personnel and their independent auditors? Many thought so. Emphasis seemed to have shifted internally at companies to increasing profits and margins by whatever means were available, and CPAs seemed more than willing to oblige by providing high-quality consulting services to meet that need. The audit took a backseat in some situations to the pursuit of higher-margin services, and raised the long-debated specter of whether these directions signaled a potential compromise to the independence of the auditor.

Whatever the future of SOX as legislation itself, the issue remains that effective accounting oversight and enforcement are critical to regaining confidence in the fairness of financial reporting, again tarnished by the exposure in 2008 and 2009 of the overly optimistic financial services industry financial reporting, and the near-collapse of major financial and industrial institutions.

We are into the period when smaller public companies are now required to report on the effectiveness of their controls over financial reporting. When their auditors begin reporting on their own assessments of client internal controls it will be a different environment than in 2003–2004, when the accelerated filers and their auditors began this process:

- True, we have more experience as a business and audit community in understanding the requirements and how to go about the assessment process.
- True, we have the benefit of clarifying guidance that removes some of the specific guidance that some believe prompted unnecessary work.
- However, many of the 12,000-plus nonaccelerated filers are not "deep" in resources such as internal audit departments and dedicated IT audit staff. Some struggle to cover basic accounting and reporting competency requirements.
- The suspicion is that the smaller companies have fewer effective controls in place.
- Based on comments by a PCAOB staff, more than 1,000 of these companies are audited by CPA firms with only one or two public clients, and thus neither the client nor the auditor have in-house experience to call on.

Costs and Results

There have now been some studies of factors that influence the costs of Sarbanes-Oxley compliance. In one study of 2,451 accelerated filers that reported on the effectiveness of their internal controls in both 2004 and 2005,[1] some findings are worthy of note:

- The smaller of the accelerated filers in this group reported a greater proportion of the material weaknesses. This may have implications for the nonaccelerated filers.
- Audit fees were relatively higher for companies reporting a material weakness.
- Audit fees generally declined in the second year of implementation. Greater reductions were found in companies with effective internal controls in the second or both years.
- The audit fees for companies reporting a material weakness in the second year increased.

EFFECTIVENESS OF THE REGULATIONS Anecdotal evidence and information gathered for an academic research study[2] identify many deficiencies in internal control in even the largest and most well-controlled entities. In a study of 44 accelerated filer audit engagements over two years (2004 and 2005) that yielded 76 data observations, around 4,000 deficiencies of various magnitudes were identified and documented by entities and auditors. It was found that management's classification of the severity of deficiencies that were also assessed by the auditor were often understated, adding credence to the value of independent auditor involvement. Also, the auditor seems to have been the primary source of deficiency identification (over 70 percent of the total deficiencies) and control tests were the predominant discovery vehicle for uncovering the deficiencies (over 80 percent). The remediation of material weaknesses identified during the year resulted in a more modest reported number of ineffective control opinions than would have been the case if all weakness (and not just those remaining at year-end) were determinant of controls effectiveness. By that measure, the requirements seem to be identifying issues that should result in fewer financial statement misstatements and restatements.

Evidence also shows that after an initial rise in restatements after the introduction of the internal controls requirements (i.e., a number of past misstatements were uncovered by the procedures), subsequent years show a decline and leveling off of the upward trends of pre-Sarbanes years. Also, some studies show that a lower cost of capital is associated with companies with effective internal controls. A 2008 report of the Association of Certified Fraud Examiners noted that companies that implemented such antifraud controls as a fraud hotline experienced over 60 percent lower loss due to

fraud. The implementation of other controls and audit-related procedures also revealed significant reductions in the losses due to fraud. Clearly gains are being made. But the cost-benefit remains in debate. While the lessened requirements of the SEC's guidance[3] and the new PCAOB Auditing Standard Number 5: An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements[4] are designed to enhance efficiency, the intent is to not lessen the effectiveness of the intended legislation for companies and auditors.

AREAS OF CONTROL WEAKNESSES Information is also available from various sources and from research on the types of discovered control problems that eventually led to a conclusion that controls were ineffective due to one or more material weaknesses. Time and again the most significant factor leading to the ineffective controls conclusion and report was finding the control problem too late in the audit process to effectively remediate the control or even after the end date of the financial statements when remediation as of the reporting date is impossible. The timing of the finding, more than the nature or other character of the deficiency, seems to be a big factor in the reporting of a weakness. Problems in the period end close process and the tax accrual process were often discovered after the fiscal year end. Problems in information technology and the control environment were potentially fixable had these problems been discovered on a timely basis instead of companies and auditors waiting until the last minute to evaluate these controls. This finding has very significant implications for companies and auditors who procrastinate or underestimate what it will really take to accomplish the required controls assessments.

Management's Evaluation of Internal Control

The Sarbanes-Oxley Act of 2002 (SOX) made significant changes to many aspects of the financial reporting process. One of those changes is a requirement that management provide a report that contains an assessment of an entity's internal control over financial reporting.

Securities and Exchange Commission (SEC) rule 13a-15 (f) defines internal control over financial reporting in this way:

> *The term internal control over financial reporting is defined as a process designed by, or under the supervision of, the issuer's principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer'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:

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

When considering the SEC's definition, you might consider:

- The term "internal control" is a broad concept that extends to all areas of the management of an enterprise. The SEC definition narrows the scope of an entity's consideration of internal control to the preparation of the financial statements, hence the use of the term "internal control *over financial reporting*." However, the lines of demarcation are not as bright and sharp as one might like them to be. The 1992 COSO Framework document identified three basic segments of control—operations, financial reporting, and regulation. While our focus is on financial reporting, operations problems can impact allowances and warranty estimates that become financial reporting issues. Failure to comply with laws and regulations or changing laws and regulations can create contingencies that require financial statement disclosures. Thus, while the focus is financial reporting, the sources of influences are not restricted.
- The SEC intends its definition to be consistent with the definition of internal controls that pertain to financial reporting objectives that was provided in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Report. (See Chapter 2 of this book for a detailed discussion of the COSO Report.)

Unless otherwise indicated, this book uses the term "internal control" to mean the same thing as "internal control over financial reporting," as defined by the SEC rules.

Management files its internal control report together with the annual 10-K. The internal control report must include:[5]

A. *Management's Annual Report on Internal Control over Financial Reporting*. Provide a report on the company's internal control over financial reporting that contains:
   1. A statement of management's responsibilities for establishing and maintaining adequate internal control over financial reporting
   2. A statement identifying the framework (e.g., COSO) used by management to evaluate the effectiveness of the company's internal control over financial reporting
   3. Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. This discussion must include disclosure of any material weakness in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting.

B. *Attestation Report of the Registered Public Accounting Firm*. Provide the registered public accounting firm's opinion on the effectiveness of a company's internal control over financial reporting. The public accountant's report on internal control for nonaccelerated filer clients was to begin for reports filed on or after December 15, 2009, but yet a further delay until the filing of reports for fiscal years ending on or after June 15, 2010 was announced in October, 2009 to provide more time for companies to efficiently comply with the requirements. However, companies should keep abreast of latest developments through their securities counsel.

C. *Changes in Internal Control over Financial Reporting*. Disclose any change in the company's internal control over financial reporting that has materially affected, or is reasonably likely to materially affect the company's internal control over financial reporting.

Overview of the Evaluation Process

While deferred from an initial "start date" of 2005, nonaccelerated filer public companies are currently required to attest annually to the effectiveness of their controls.

SEC Release Nos. 33-8810 and 34-55928 provide important interpretative guidance for management regarding its evaluation of internal control. The SEC rules on evaluating internal control are objective-driven and principles-based, and they start with a description of the overall objective of management's evaluation. Having a clear understanding of the overall objective of your evaluation is vital if you want that process to be as effective and efficient as possible.

Management must have a "reasonable basis" for its annual assessment. To provide this reasonable basis, management must perform an annual evaluation of internal control.

According to the SEC, the primary objective of management's evaluation is to:

> *Provide management with a* reasonable basis *for its annual assessment as to whether any* material weaknesses *in internal control exist as of the end of the fiscal year.*

The phrases in italics are of critical importance in planning and performing an evaluation of internal control. Unfortunately, these terms are conceptual and not subject to fine-line distinctions.

- *Reasonable basis.* A reasonable basis is "such level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs." The notion of "reasonable" does not imply an unrealistic degree of precision or a single conclusion or evaluation approach. By setting a threshold of "reasonableness" to its guidance, the SEC acknowledges that management can and should exercise judgment in how it complies with its rules and that there is some range of appropriate ways to evaluate internal control.
- *Material.* An amount is material to the financial statements if it would change or influence the judgment of a financial statement user. Note that the SEC rules direct management to identify "material weaknesses," not all weaknesses or deficiencies in internal control. Having a clear understanding of what is and is not material will help you assess the severity of control issues identified and make defensible judgments on what accounts, balances, and classes of transactions should be included in the scope of the assessment. The term "material" in discussions of internal control is the same as in the preparation of the financial statements.

Even though the SEC has provided interpretative guidance, ultimately this guidance not only allows for but actively encourages management to exercise its judgment in the design and execution of the procedures it performs to meet the overall objective for evaluating internal control.

While this flexibility is positioned as an opportunity to perform an efficient assessment, the "two-edged sword" is an ineffective assessment that could be the result of unsupported risk assessments.

MATERIAL WEAKNESS AND SIGNIFICANT DEFICIENCY The SEC states that an overall objective of the evaluation of internal control is to determine whether a material weakness exists as of the fiscal year-end. In order to meet this objective, it is critical to have a working definition of the term.

A *material weakness* is a *deficiency*, or combination of deficiencies, in internal control such that there is a *reasonable possibility* that a material misstatement of the annual or interim financial statements will not be prevented or detected in a timely basis.

A control *deficiency* exists 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.

There is a *reasonable possibility* of an event when the likelihood of the event is more than remote. This statement is in the context of FASB Statement No. 5, *Accounting for Contingencies*, where these conceptual terms are used.

One change brought about by the revised SEC and PCAOB guidance is the use of the term "reasonably possible" in the definition of material weaknesses. Prior guidance used the term "more than remote," which some felt focused too much attention on the "remote" term and resulted in identifying more material weaknesses than appropriate. Be not misled—the new definition says the same thing as the old one; "reasonably possible" has exactly the same meaning as "more than remote" in the context of FAS 5. So why the change? One view is that it is a cosmetic change and not one of substance.

A very practical implication of the definition that has sometimes eluded companies and auditors is that a material misstatement is not required to identify a deficiency as a material weakness. For example, if there is no effective control over cash disbursements, accounting personnel may effectively process transactions correctly, but from a controls perspective, the controls gap is likely to be a material weakness if a material volume of transactions flow through that accounting process.

A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of a registrant's financial reporting.

An issue relevant to the material weakness and significant deficiency determinations is that they remain a subjective judgment and reasonable persons might disagree on the severity assessment in some situations. The implications of hindsight and second guessing "in times of trouble" are certainly an exposure that companies and auditors need to consider when working with these imprecise definitions.

SEC Company Requirements

In the early days of company experience with SOX there was little direct guidance available on company requirements except for a few broad

statements that were part of the legislation itself. In contrast, the PCAOB provided surprisingly specific guidance to auditors regarding the conduct of their examinations of company assessments and their own examinations of the effectiveness of their client's internal controls. This led to the interesting suggestion that companies study the requirements laid out for auditors in order to better understand their requirements. Throughout 2004, both the SEC and the PCAOB responded to questions by both registrants and their auditors and issued a series of question-and-answer documents, interpreting the guidance to date and filling in some of the "holes" in the guidance.

A positive step in 2007 was the SEC's issuance of additional guidance in SEC Release No. 33-8810 and the PCAOB's overhaul of its Auditing Standard and reissuance as Auditing Standard No. 5. While the SEC guidance added clarity to the requirements for companies, AS 5 reduced the specificity of the guidance for auditors, allowing for much more judgment in the nature, timing, and extent of procedures to be applied and in the judgments concerning the severity of deficiencies. The concerns about the cost of compliance and numerous anecdotal stories of "over-the-top" auditing led to guidance fairly heavily weighted in judgment over process.

Nevertheless, a critical question that arises when discussing SOX requirements is "What do I have to do?" SEC Release No. 33-8810 is an excellent source for answering this question. Selected excerpts from this release are classified by phases and subheadings in the assessment process for ease of understanding. Page references in that SEC guidance (downloadable from the SEC Web site) are also included for convenience.

Planning and Scope of Assessment

The SEC in Release 33-8810 has directed a number of comments to specific issues that companies need to be aware of. These comments are found in different sections of the SEC guidance but are organized here by subject for reader convenience. This book often quotes the SEC language when the SEC speaks on a specific topic or issue. Readers should be alert to comments by the author, as distinguished from SEC guidance.

> *Management is responsible for maintaining a system of internal control over financial reporting ("ICFR") that provides reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. [SEC Release 33-8810, page 2]*
>
> *Under the Commission's rules, management's annual assessment of the effectiveness of ICFR must be made in accordance with a suitable*

control framework's definition of effective internal control. [SEC Release 33-8810, page 11].

While the COSO Framework is not the only means to satisfy the requirements (other frameworks include COCO in Canada and the Turnbull Report in the U.K., and are close in content to the COSO Framework), COSO is the best known by the business community and auditors and is more likely to result in efficiencies in selecting and developing internal tools and working with independent auditors. "SOX in Japan" is unlikely to meet SEC requirements since its scope is less.

. . . management's evaluation would ordinarily consider evidence from a reasonable period of time during the year, including the fiscal year-end. [SEC Release 33-8810, page 29]

This sentence actually broadens and for some clarifies the focus of the requirements. Since the attestation is as of a point in time (the balance sheet date), it has been reasoned that controls only need to be assessed as effective at or near the period-end. However, the disconnect between the point in time assessment and the intent of SOX to provide effective internal control over financial reporting, which takes place over a period of time such as in quarterly reporting or in reporting significant events during the year, is becoming more evident.

Management's consideration of financial reporting risks generally includes all of its locations or business units. Management should generally consider the risk characteristics of the controls for each financial reporting element, rather than making a single judgment for all controls at that location when deciding whether the nature and extent of evidence is sufficient. [SEC Release 33-8810, pages 32–33].

This requirement clarifies that broad scoping assessments such as simply targeting the largest entity units or subsidiaries, or gathering some target percentage (e.g., 80 percent) of the income, assets, or revenues may not lead to acceptable results.

We believe the principles-based guidance permits flexible and scalable evaluation approaches that will enable management of smaller public companies to evaluate and assess the effectiveness of ICFR without undue cost burdens. However, the flexibility provided in the guidance is not meant to imply that evaluations for smaller public companies be conducted with less rigor, or to provide anything less than reasonable assurance as to the effectiveness of ICFR at such companies. [SEC Release 33-8810, page 50]

It is clear that a reduction in effectiveness is not intended in any of the modifications to past company practice and SEC guidance. Companies will be held to a high standard of assessment quality and should plan on approaching the assessment with the serious intent of identifying financial reporting risks and performing effective procedures to support their assessment.

> *. . . foreign private issuers should scope their evaluation effort based on the financial statements prepared in accordance with home country GAAP, rather than based on the reconciliation to U.S. GAAP. [SEC Release 33-8810, page 75]*

When financial reporting under U.S. GAAP differs from the accounting required in the U.S., then local accounting determines the basis for assessing the significance of an audit area. For example, if sales of a product in a local country can be recorded earlier than under GAAP, then the larger (local) sales value should be the basis of assessing the area for scoping purposes. However, since the reconciliation to U.S. GAAP may be itself a significant process, care should be taken to assess whether the controls over the reconciliation process are to be included in the scope of the assessment.

PERFORMANCE OF THE ASSESSMENT

Support and Documentation The following SEC paragraphs outline the documentation and support requirements for management assessments.

> *Management is responsible for maintaining evidential matter, including documentation, to provide reasonable support for its assessment. [SEC Release 33-8810, page 2]*
>
> *As part of its evaluation of ICFR, management must maintain reasonable support for its assessment. [SEC Release 33-8810, page 38] Documentation of the design of the controls management has placed in operation to adequately address the financial reporting risks, including the entity-level and other pervasive elements necessary for effective ICFR, is an integral part of the reasonable support. [SEC Release 33-9810, page 20]*
>
> *The documentation does not need to include all controls that exist within a process that impacts financial reporting. Rather, the documentation should be focused on those controls that management concludes are adequate to address the financial reporting risks. [SEC Release 33-8810, page 21]*
>
> *Reasonable support for an assessment would include the basis for management's assessment, including documentation of the methods and*

procedures it utilizes to gather and evaluate evidence. [SEC Release 33-8810, page 31]

Smaller companies . . . documentation might include memoranda, e-mails, and instructions or directions to and from management to company employees. [SEC Release 33-8810, page 32]

The issue of documentation is recurring throughout the release. One of the key stumbling blocks companies often encounter is identifying what is "adequate" documentation. This has a huge impact on efficiency since documenting "everything that moves" is unnecessary and makes the documentation impractical to maintain in future periods. Careful consideration of the COSO documentation guidance (discussed later in this book) can be a very worthwhile investment in time when balancing documentation completeness with efficiency. Adequate and not excessive documentation that conforms to COSO guidelines will also facilitate review by the independent auditor and help control audit costs. In the author's view, the lack of a specified or widely used format for documentation is a contributing factor to inefficiencies in compliance, since each company must invent on its own the format that to its understanding at the time meets the requirements.

Risk Assessment These key SEC statements form the risk assessment guidance for companies.

The first principle is that management should evaluate whether it has implemented controls that adequately address the risk that a material misstatement of the financial statements would not be prevented or detected in a timely manner. [SEC Release 33-8810, page 4]

The second principle is that management's evaluation of evidence about the operation of its controls should be based on its assessment of risk. [SEC Release 33-8810, page 5]

The evaluation begins with the identification and assessment of the risks to reliable financial reporting (that is, materially accurate financial statements), including changes in those risks. Management then evaluates whether it has controls placed in operation (that is, in use) that are designed to adequately address those risks. [SEC Release 33-8810, page 12]

Ordinarily, the identification of financial reporting risks begins with evaluating how the requirements of GAAP apply to the company's business, operations and transactions. [SEC Release 33-8810, page 12]

Management may find it useful to consider "what could go wrong" within a financial reporting element in order to identify the sources and the potential likelihood of misstatements and identify those that could

result in a material misstatement of the financial statements. [SEC Release 33-8810, page 13]

These characteristics include, among others, the size, complexity, and organizational structure of the company and its processes and financial reporting environment, as well as the control framework used by management. [SEC Release 33-8810, page 13]

Management's evaluation of the risk of misstatement should include consideration of the vulnerability of the entity to fraudulent activity.... Management should recognize that the risk of material misstatement due to fraud ordinarily exists in any organization, regardless of size or type, and it may vary by specific location or segment and by individual financial reporting element. [SEC Release 33-8810, page 14]

Management's consideration of the misstatement risk of a financial reporting element includes both the materiality of the financial reporting element and the susceptibility of the underlying account balances, transactions or other supporting information to a misstatement that could be material to the financial statements. [SEC Release 33-8810, page 25]

Financial reporting elements that involve related party transactions, critical accounting policies, and related critical accounting estimates generally would be assessed as having a higher misstatement risk. [SEC Release 33-8810, page 26]

... manual controls would be assessed as higher risk [SEC Release 33-8810, page 27]

Risk assessment is the heart of the controls assessment process since failing to identify a risk could mean failing to detect a material weakness that may someday result in a material misstatement. Risk assessment is deeper than responding to known misstatements, but assessing "what *could* go wrong" and identifying controls that would prevent or detect a material misstatement. It is more than a "breezy" assessment and not necessarily a structured scorecard assessment. The point often missed is that there should be a substantive *basis* for saying an area or account is less than high risk. What evidence is there that the risk is low (and do not say it is only because you never saw a problem in this area)? A second point is the need to consider these risks "in the absence of controls" (auditors call this inherent risk) since the purpose of the assessment is to determine whether controls should be in place and tested as a basis for the assessment. Many managers and auditors have difficulty separating inherent risks and control risks in their risk assessment, since it is natural to consider them together in day-to-day thinking.

Entity-Level Controls and the Control Environment Control environment factors have been the subject of mixed messages. While critically important to the

entity, and a potential "trump card" to the ability of management to assess the operation of more detailed controls as effective, when they are ineffective, control environment factors such as effective corporate governance (e.g., boards and audit committees) are not necessarily an effective substitute for the effectiveness of controls over detailed transactions. Inherently, one could reason that the effort to assess controls when the control environment is effective should be less than when the control environment is ineffective, but the mechanism for tying the control environment to the other tests and assessments is elusive. Some have posited that an effective control environment is already assumed in the levels of testing that are commonly seen in company assessments and auditor testing.

Another aspect of entity-level controls concerns those controls with wide application across the entity, such as the use of common software and control procedures. Certainly, these procedures can be designed at a level of precision to effectively prevent or detect material misstatements. However, the lumping of control environment and these entity-level controls into the same category can create some confusion.

In the words of the SEC:

> *The more indirect the relationship to a financial reporting element, the less effective a control may be in preventing or detecting a misstatement. [SEC Release 33-8810, page 18]*
>
> *However, a strong control environment would not eliminate the need to evaluate the operation of the control in some manner. [SEC Release 33-8810, page 27]*
>
> *Entity-level controls may be designed to operate at the process, application, transaction or account-level and at a level of precision that would adequately prevent or detect on a timely basis misstatements in one or more financial reporting elements that could result in a material misstatement of the financial statements. [SEC Release 33-8810, page 19]*
>
> *However, it is unlikely that management will identify only this type of entity-level control as adequately addressing a financial reporting risk identified for a financial reporting element. [SEC Release 33-8810, page 18]*

Information Technology General Controls IT general controls, like the control environment, can be viewed as a "trump card" over reliance on automated procedures and controls when the general controls are ineffective. The normal state is an expectation that they are effective and will support testing and reliance of the detailed controls that rely on systems. Experience tells us that the most sensitive of the general controls is the security and access component. With weaknesses in security and access controls, detailed controls

can be overridden and reliance on the systems to perform their assigned functions cannot be assured.

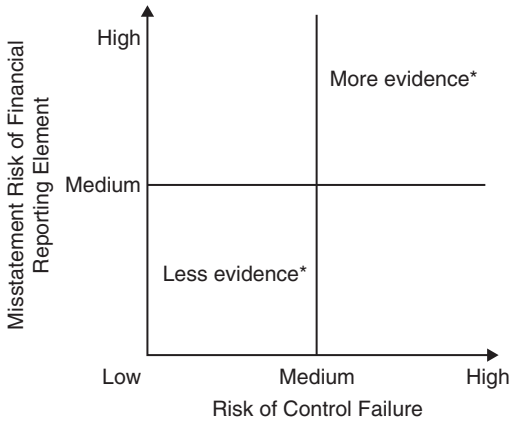
> *While IT general controls alone ordinarily do not adequately address financial reporting risks, the proper and consistent operation of automated controls or IT functionality often depends upon effective IT general controls. [SEC Release 33-8810, page 19]*
>
> *The identification of risks and controls within IT should not be a separate evaluation. Instead, it should be an integral part of management's top-down, risk-based approach to identifying risks and controls and in determining evidential matter necessary to support the assessment. [SEC Release 33-8810, pages 19–20]*

Gathering and Evaluating Evidence

Management needs a basis for its assessment, which includes evidence based on observations, inquiries, tests of controls, and examination of documents, logs, or other evidence supporting the assessment. Higher-risk areas warrant more evidence concerning the effectiveness of controls. For example, if revenue recognition is an area of risk due to the complexity of the determination of when revenue recognition is supported under GAAP, there is an expectation that more testing effort and evidence will be gathered for that area than a lower-risk, less significant, and simpler area such as accounting for prepaid insurance costs. Exhibit 1.1 is a chart from the SEC 8810 guidance (page 24) indicating the relationship between misstatement risk and the required evidence.

While auditing principles for private entities accept the concept of rotation of controls testing over no more than three years,[6] the SEC makes clear that a formal rotation of areas is not considered appropriate in public company controls assessment; however, it is acceptable and encouraged that testing of controls may vary in intensity from period to period.

> *Management should evaluate evidence of the operating effectiveness of ICFR. [SEC Release 33-8810, page 21]*
>
> *Evidence about the effective operation of controls may be obtained from direct testing of controls and on-going monitoring activities. [SEC Release 33-8810, page 22]*
>
> *The evidential matter constituting reasonable support for management's assessment would ordinarily include documentation of how management formed its conclusion about the effectiveness of the company's entity-level and other pervasive elements of ICFR that its applicable framework describes as necessary for an effective system of internal control. [SEC Release 33-8810, page 32]*



*The references to "more" or "less" include both the quantitative and qualitative characteristics of the evidence (that is, its sufficiency).

EXHIBIT 1.1 Determining the Sufficiency of Evidence Based on ICFR Risk

. . . management cannot decide to include controls for a particular location or process within the scope of its evaluation only once every three years or exclude controls from the scope of its evaluation based on prior year evaluation results. To have a reasonable basis for its assessment of the effectiveness of ICFR, management must have sufficient evidence supporting the operating effectiveness of all aspects of its ICFR as of the date of its assessment. [SEC Release 33-8810, page 62]

REPORTING AND CONCLUDING As stated by the SEC:

If management determines that the operation of the control is not effective, a deficiency exists that must be evaluated to determine whether it is a material weakness. [SEC Release 33-8810, page 30]

A deficiency in the design of ICFR exists when (a) necessary controls are missing or (b) existing controls are not properly designed so that, even if the control operates as designed, the financial reporting risks would not be addressed. [SEC Release 33-8810, page 15]

Management may not disclose that it has assessed ICFR as effective if one or more deficiencies in ICFR are determined to be a material weakness. As part of the evaluation of ICFR, management considers whether each deficiency, individually or in combination, is a material weakness as of the end of the fiscal year. [SEC Release 33-8810, page 34]

> *Under COSO, risk assessment and monitoring are two of the five components of an effective system of internal control. If management concludes that an internal control component is not effective, or if required entity-level or pervasive elements of ICFR are not effective, it is likely that internal control is not effective. [SEC Release 33-8810, page 72]*

This seems to be a long way around in saying that all five COSO components need to be effective for internal control to be effective. This is a stated principle in the COSO Framework.

> *Pursuant to Exchange Act Rules 13a-14 and 15d-14 [17 CFR 240. 13a-14 and 240.15d-14], management discloses to the auditors and to the audit committee of the board of directors (or persons fulfilling the equivalent function) all material weaknesses and significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize and report financial data. [SEC Release 33-8810, page 34]*

This requirement ensures that important information is shared within the entity and with the auditors. If deficiencies are not communicated to the auditors, auditors may not identify the deficiency in their testing and erroneously rely on the control during the period for purposes of examining the financial statements of the company. This requirement is sometimes overlooked when management identifies and remediates the control, but the requirement is not dependent on whether the control is remediated or not.

> *Management evaluates the severity of a deficiency in ICFR by considering whether there is a reasonable possibility that the company's ICFR will fail to prevent or detect a misstatement of a financial statement amount or disclosure; and the magnitude of the potential misstatement resulting from the deficiency or deficiencies. The severity of a deficiency in ICFR does not depend on whether a misstatement actually has occurred but rather on whether there is a reasonable possibility that the company's ICFR will fail to prevent or detect a misstatement on a timely basis. [SEC Release 33-8810, page 35]*
>
> *Management should evaluate the effect of compensating controls when determining whether a control deficiency or combination of deficiencies is a material weakness... Compensating controls are controls that serve to accomplish the objective of another control that did not function properly, helping to reduce risk to an acceptable level. [SEC Release 33-8810, page 37]*

Care needs to be taken not to ascribe significant precision to certain monitoring or other compensating controls when such reliance is not supported by analysis and evidence. If the compensating control should have operated on a material misstatement that was identified, and it did not identify or correct the misstatement, it is hard to argue such a compensating control is effective.

Management should evaluate whether the following situations indicate that a deficiency in ICFR exists and, if so, whether it represents a material weakness (from SEC Release 33-8810):

- *Identification of fraud, whether or not material, on the part of senior management [page 50]*
- *Restatement of previously issued financial statements to reflect the correction of a material misstatement [page 51]*
- *Identification of a material misstatement of the financial statements in the current period in circumstances that indicate the misstatement would not have been detected by the company's ICFR*
- *Ineffective oversight of the company's external financial reporting and internal control over financial reporting by the company's audit committee [page 37]*

These four situations do not necessarily equate to material weaknesses, but careful reasoning is necessary if they are not assessed as such. The presumption is that in most cases they will be assessed as material weaknesses. AS 2 had even stronger wording supporting material weakness treatment for these situations.

> *In addition, if a material weakness exists, management may not state that the company's ICFR is effective. However, management may state that controls are ineffective for specific reasons. [SEC Release 33-8810, page 38]*
>
> *The goal underlying all disclosure in this area is to provide an investor with disclosure and analysis that goes beyond describing the mere existence of a material weakness. [SEC Release 33-8810, page 39]*

Management is expected to explain the nature of the material weakness, if one exists, in its reporting on internal control.

> *The Commission's disclosure requirements state that management's annual report on ICFR must include a statement as to whether or not ICFR is effective and do not permit management to issue a report on ICFR with a scope limitation. [SEC Release 33-810, page 41]*

The reporting scenario is fairly simple—controls are or are not effective. The SEC does not support "except for" conclusions nor conclusions citing a scope limitation. If fire, flood, or pestilence prevents the assessment of essential controls, then controls should not be assessed as effective.

AUDITOR REVIEW OF MANAGEMENT'S ASSERTION Auditors no longer (under AS 5) have to specifically report on management's process and report on internal controls. However, the SEC and PCAOB have made reference to the general audit requirement that auditors read management discussions and disclosures and say something if they find them to be unsupported or misleading. The documentation of your project provides evidence to the auditor that you have a reasonable basis for your assertion regarding internal controls effectiveness.

What this means is that auditor will make an assessment of what you did and how you did it, and if the process is ineffective and evidence is not sufficient for management to conclude, the auditor will ask management modify its assertion or the auditor will have to make a comment. From the SEC Release No 33-8809:

> *Despite the fact that the revised rules no longer require the auditor to separately express an opinion concerning management's assessment of the effectiveness of the company's ICFR, auditors currently are required under Auditing Standard No. 2 ("AS No. 2") and would continue to be required under the Proposed Auditing Standard, to evaluate whether management has included in its annual ICFR assessment report all of the disclosures required by Item 308 of Regulations S-B and S-K. Both AS No. 2 and the Proposed Auditing Standard would require the auditor to modify its audit report on the effectiveness of ICFR if the auditor determines that management's assessment of ICFR is not fairly stated. Consequently, the revisions are fully consistent with, and will continue to achieve, the objectives of Section 404(b) of Sarbanes-Oxley. [SEC Release 33-8810, Page 12]*

The PCAOB in AS 5 states:

> *73. If the auditor determines that any required elements of management's annual report on internal control over financial reporting are incomplete or improperly presented, the auditor should follow the direction in paragraph C2. . .*
>
> *C2.* Elements of Management's Annual Report on Internal Control Over Financial Reporting Are Incomplete or Improperly Presented. *If the auditor determines that elements of management's annual report on*

internal control over financial reporting are incomplete or improperly presented, the auditor should modify his or her report to include an explanatory paragraph describing the reasons for this determination.

Thus, it is expected that auditors will review management's project and support for their assertion.

Use of Work of Internal Auditors and Others

Both the SEC and the PCAOB recognize that external auditors should be able to rely, to some degree, on the work performed by management in its self-assessment of internal control in their audit. This guidance is considerably relaxed from the AS 2 requirements where auditors in some areas could not take any assurance from company assessment procedures, however effectively performed. As a result, companies complained that the original guidance forced redundant and unnecessary testing. Nevertheless, the primary objective of an audit of internal controls over financial reporting is to obtain an objective, independent opinion. To form and take responsibility for such an opinion, auditors must do some of their investigation independently from the company.

We know from reported research that over 70 percent of the identified control deficiencies in 2004 and 2005 in a sample of company data were identified by the independent auditor. To what extent the redundancy of retesting client controls after the company tested and concluded effectiveness contributed to these findings cannot be known, but permitting more reliance on company testing places more importance on independent auditors making correct assessments of the objectivity and competence of company assessment and testing procedures.

Thus, companies and auditors must balance two competing goals: objectivity and independence of the parties involved versus the use of management's work by the external auditor as a means of limiting the overall cost of compliance.

For companies, the implications of this relaxation of the requirements are obvious. The more objective, rigorous, and competent the company examinations, the more reliance auditors can place on that work, significantly reducing the required time and cost associated with the audit process. For companies not yet subject to auditor opinions on internal control, the experience of earlier assessments can be used as an opportunity to "ramp up" for the eventual oversight and prepare for an efficient audit process.

Additionally, we know from research that effective controls assessments are less costly than when the controls are assessed as ineffective. A rigorous process to root out and correct deficiencies in controls design and

operation in advance of formal auditor involvement can result in compounding dividends.

EXTERNAL AUDITOR'S USE OF THE COMPANY'S INTERNAL CONTROL TESTING AND EVALUATION Ultimately, the auditor is responsible for determining the extent to which he or she will rely on management's work in the audit. PCAOB Auditing Standard No. 5 provides guidance to auditors on the principles they should use to make that determination.

Paragraph 19 of the auditing standard provides extensive guidance on the degree to which the company's work on internal control can be used by the external auditors. The relevant section is titled "Using the Work of Others." The standard indicates that the work of "others" includes the relevant work performed by:

- Internal auditors
- Other company personnel
- Third parties working under the direction of management or the audit committee

In general, the auditor's determination about using the work of others is a risk-based judgment: The greater the risk, the more the auditor will want to use more of his or her own work to form an opinion. As the risk decreases, the auditor may rely more on the work of the company.

The external auditor's ability to rely on the work of others has its limits. Paragraph 35 of the standard states that the procedures performed to achieve certain audit objectives should be performed principally by the auditor. The objectives are:

- Understanding the flow of transactions related to the relevant assertions, including how these transactions are initiated, authorized, processed, and recorded
- Identifying the points within the company's processes at which a misstatement—including a misstatement due to fraud—could arise that, individually or in combination with other misstatements, would be material
- Identifying the controls that management has implemented to address these potential misstatements
- Identifying the controls that management has implemented over the prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could result in a material misstatement of the financial statements

To achieve these objectives, the auditor typically performs a walk-through for each of the company's significant accounts and disclosures. As part of its evaluation, management also may also perform walk-throughs of these same accounts. Quality company documentation is a significant benefit to the auditor in performing these requirements. In the absence of such quality documentation, the auditor is obliged to create sufficient documentation for audit purposes. Note that the requirements are for "understanding" and "identifying" and not for documenting the controls. Companies can go a long way to cost efficiencies by having appropriate controls documentation. Considering auditor hourly rates, the economics of placing company effort to this task should be clear.

ASSESSING COMPETENCE AND OBJECTIVITY Auditors will have to assess the competence and objectivity of those people whose work they plan to use. The higher the degree of competence and objectivity, the greater use auditors may make of the work.

Competence means the attainment and maintenance of a level of understanding and knowledge that enables that person to perform ably the tasks assigned to them.

Objectivity means the ability to perform those tasks impartially and with intellectual honesty. For example, self-assessments of performance by company personnel who performed the control or performed the underlying process will generally not qualify as an objective process.

Competence and objectivity go hand in hand. The auditor will not use the work of someone who has a low degree of objectivity, regardless of the person's level of competence. Likewise, the auditor should not use the work of someone who has a low level of competence, regardless of his or her objectivity.

To allow the company's external auditors to make as much use as possible of the company's own assessment of internal control, company management should have a clear understanding of the conditions that must be met for the external auditors to use the work. To help the external auditors determine that those criteria have been met, you may wish to *document your compliance with the key requirements* of the auditing standard and make this documentation available to the external auditors early on in their audit planning process. For example, you should consider:

- Obtaining the biographies or resumes of project team members showing their education level, experience, professional certifications, and continuing education
- Documenting the company's policies regarding the assignment of individuals to various SOX work areas

- Documenting the "organizational status" of the project team and how they have been provided access to the board of directors and audit committee
- Establishing policies that ensure that the consistent and clear *documentation* of the work performed includes:
  - A description of the scope of the work
  - Work programs
  - Evidence of supervision and review
  - Conclusions about the work performed

Working with the Independent Auditors

To render an opinion on either the financial statements or the effectiveness of internal control, the company's independent auditors are required to maintain their independence, in accordance with applicable SEC rules. These rules are guided by certain underlying principles, which include:

- The audit firm must not be in a position where it audits its own work.
- The auditor must not act as management or as an employee of the client.

For example, with regard to internal controls, the auditor could not design or implement a system of internal controls and still be sufficiently independent to perform an audit of those controls.

Since the early days of SOX, the SEC has relaxed some of the strict limitations on auditor's involvement in the company's controls assessment and testing process. Nevertheless, the more involved the independent auditor is in the company project, the more likely independence conflicts will arise. There seems to be no debate that the auditor could assist in documenting controls under the supervision of company leadership. The inverse arrangement is not likely to be acceptable. While the auditor can rely on some of management's testing for its assurance, the company is not to rely on auditor testing as a basis for their assessment, which should stand on its own. Under the COSO Framework, the independent auditor is not a component of the company's internal control and should not be a source of direct testing or monitoring that is required of companies.

The auditor's rules of independence require the audit committee to preapprove any nonaudit services related to internal control over financial reporting. In seeking this preapproval, the auditor will:

- Provide a written description of the scope of the internal control–related services to the audit committee

- Discuss with the audit committee the potential effects of the service on the independence of the firm
- Document the substance of its discussion with the audit committee

Companies seeking assistance in assessing, documenting, and testing controls have often sought assistance from consultants and audit firms other than the independent auditor firm to avoid independence concerns.

A violation of independence rules in this regard can have significant consequences such as the disqualification of the auditor from issuing an opinion on both the internal controls and the financial statements.

Notes

[1] Jean C. Bedard, Lynford Graham, Rani Hoitashi, and Udi Hoitashi. "Sarbanes-Oxley Section 404 and Internal Controls," *CPA Journal*, October 2007.

[2] Jean C. Bedard and Lynford Graham. *Archival Evidence on Detection and Severity Classification of Sarbanes-Oxley Section 404 Internal Control Deficiencies, and Archival Evidence on Remediation of Sarbanes-Oxley Section 404 Internal Control Deficiencies Bentley University. Working Papers 2009.*

[3] Securities and Exchange Commission. *Commission Guidance Regarding Management's Report on Internal Control over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934.* Release Nos. 33-8810; 34-55929; FR-77; File No. S7-24-06.

[4] Public Company Accounting Oversight Board. Auditing Standard Number 5. *An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements.* PCAOB Release No. 2007-005. May 24, 2007.

[5] See Regulation S-K, Item 308 (17 CFR §229.308).

[6] The concept of rotation of controls involves the reliance on tests of control performed in period one, for up to two more years, provided there is no apparent change in controls or personnel performing the control. The AICPA guidance for nonpublic entities still requires an assessment of the controls design and some evidence the control is still operating to support reliance on prior year tests. There is no specific SEC guidance on how or when to vary the intensity of testing controls effectiveness from year to year.