Reform of the Sarbanes-Oxley Section 404 Internal Control over Financial Reporting Regime

James Hamilton, J.D., LL.M.

CCH Principal Analyst

Table of Contents

Introduction

With Congress closely watching, the SEC and PCAOB have worked together to create a new risk-based, principles-based regime for reporting on the effectiveness of internal control over financial reporting pursuant to Section 404 of the Sarbanes-Oxley Act. Section 404, of course, remains unchanged, but the rules, guidance, and standards promulgated pursuant to the statute have been reformed in response to concerns that internal controls compliance was overly costly and harmful to the competitiveness of U.S. financial markets. The reforms build on the guidance issued by the SEC and PCAOB in May of 2005 (see FED. SEC. L. REP. ¶¶87,411 and 87,413).

The SEC has issued management guidance and amended a number of internal controls rule (see press release 2007-101 (May 23, 2007)). For its part, the PCAOB adopted a new Auditing Standard No. 5 on the audit of internal control over financial reporting, to replace Auditing Standard No. 2, and adopted a rule requiring audit committee pre-approval of non-audit internal control services (see PCAOB Release No. 2007-005 (May 24, 2007)).

The effective date of the SEC interpretive guidance and adopted rules will be 30 days from their publication in the Federal Register. The Board's new auditing standard is subject to Commission approval and, when approved, is expected to take effect no later than for calendar year 2007 audits, with early adoption encouraged. SEC approval of AS 5 is expected to be expeditious.

Purpose and Objectives

The primary purpose of internal control over financial reporting is to foster the preparation of reliable and accurate financial statements. Thus, the overarching principle of the new regulatory regime is that internal controls must be designed and implemented to prevent or detect material misstatements in the company's financial statements. In other words, the edifice of internal control mandates is aimed at ensuring that the company's SEC-filed financial statements are accurate and fairly present the company's financial condition and results of operation.

The risk in the risk-based approach is the risk of a material misstatement in the financial statements. One of the great principles in this principles-based regime is that the auditor should vary the control testing to respond to the risk. Experience under the old regime demonstrated that areas posing the greatest danger of material misstatement can be obscured when internal controls are audited without adequate consideration of risk.

Although the SEC incorporated certain sections of the May 2005 staff guidance into the new interpretive guidance, the Commission emphasized that the staff guidance remains relevant. Thus, companies that have already completed one or more evaluations can continue to use their existing procedures to satisfy the evaluation required by the new SEC rules, or companies can choose to follow the guidance. The guidance and rules are intended to make implementation of

the internal control reporting requirements more efficient and cost-effective by reducing ambiguities that have arisen due to the lack of certainty available to companies on how to conduct an annual evaluation of internal controls.

The SEC has worked with the PCAOB staff to closely align their respective positions. In this spirit, the guidance aligns the definition of “material weakness” and the related guidance for evaluating deficiencies, including the indicators of a material weakness.

The SEC similarly improved the alignment around guidance for evaluating whether controls adequately address financial reporting risks, the factors to consider when identifying financial reporting risks, and the factors for assessing the risk associated with individual financial reporting elements and controls. These represent areas of key judgment for both management and auditors in determining whether the internal controls are effective and in determining the nature, timing and extent of evaluation and audit procedures.

Even so, some differences are expected to remain between the SEC’s management guidance and the PCAOB’s new audit standard. These differences are not necessarily contradictions or misalignment, explained the SEC, rather they reflect the fact that management and the auditor have different roles and duties with respect to evaluating and auditing internal controls over financial reporting.

Management’s daily involvement with its internal control system provides it with knowledge and information that may influence its judgments about how best to conduct the evaluation and the sufficiency of evidence it needs to assess the effectiveness of the internal controls. Differences in the respective approaches are likely to exist because the auditor does not have the same information and understanding as management, as well as because the auditor will integrate its tests of internal controls with the financial statement audit.

According to Chairman Christopher Cox, the management guidance enables companies of all sizes to reduce compliance costs by scaling and tailoring their evaluation procedures according to their facts and circumstances. The guidance also enables companies of all sizes to focus on what truly matters to the integrity of the financial statements, risk and materiality, said Conrad Hewitt, SEC Chief Accountant. By providing management with its own guidance for evaluating internal control over financial reporting, the SEC seeks to ensure an appropriate balance between management’s evaluation process and the audit process.

PCAOB Chair Mark Olson noted that AS 5 reinforces the Board’s expectation that the integrated audit will be conducted in a manner that eliminates procedures that are unnecessary to an effective audit of internal control and increases the likelihood that material weaknesses will be found before they allow material misstatements to occur.

Overview

The management guidance, rules, and standard reform the internal control reporting system by:

- Focusing the audit on the matters most important to internal control by directing the auditor to test the most important controls
- Adopting a flexible principles-based system reliant on professional judgment
- Eliminating the requirement that the auditor evaluate management's process
- Scaling the audit for smaller companies
- Aligning SEC regulations with the PCAOB standard
- Eliminating the principal evidence provision to allow more reliance on the work of others
- Redefining material weakness upward
- Requiring audit committee pre-approval of non-audit internal control services
- Placing the main testing focus on entity or company level controls
- Requiring auditors to assess the risk of fraud when planning the audit
- Reducing the number of walkthroughs while preserving quality
- Integrating internal control and financial statement audits
- Requiring risk assessment at each of the decision points in a top-down approach
- Testing controls important to assessing the risk of financial statement misstatement
- Allowing a risk-based approach for auditing multiple corporate locations
- Allowing auditors to use knowledge obtained during past audits
- Refocusing internal controls to prevent material misstatements in financial statements

Section 404 and Its Implementation

Sarbanes-Oxley Act Section 404 is a two-prong statute requiring that annual reports filed with the SEC:

- Must be accompanied by a statement by company management that management is responsible for creating and maintaining adequate internal control over financial reporting. Management must also present its assessment of the effectiveness of those controls.

- In addition, the company's independent auditor must report on and attest to management's assessment of the company's internal controls.

On June 5, 2003, the Commission adopted rules implementing Section 404 with regard to management's obligations to report on its internal control structure and procedures and, in so doing, created the term "internal control over financial reporting." (Release No. 33-8238 (SEC 2003), FED. SEC. L. REP. ¶86,923.) The rules embody two broad principles: (1) that the evaluation must be based on procedures sufficient both to evaluate the design and to test the operating effectiveness of internal controls; and (2) that the assessment, including testing, must be supported by reasonable evidential matter. Instead of providing specific guidance at that time regarding the evaluation, the SEC expressed its belief that the methods of conducting evaluations of internal controls will, and should, vary from company to company and will depend on the circumstances of the company and the significance of the controls.

The new guidance reaffirms the SEC's belief that it is impractical to prescribe a single methodology that meets the needs of every company. Rather, management must bring its own experience and informed judgment to bear in order to design an evaluation process that meets the needs of its company and that provides reasonable assurance for its assessment. The guidance is intended to allow management the flexibility to design such an evaluation process.

To facilitate comparison of assessment reports among companies, the SEC rules implementing Section 404 require management to base its assessment of a company's internal control on a suitable evaluation framework. While the rules do not mandate a suitable framework, the SEC has indicated that the internal control integrated framework created by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) is an example of a suitable framework. The guidance is not intended to replace or modify the COSO framework.

The SEC has pointed out that the COSO framework does not set forth an approach for management to follow in evaluating the effectiveness of a company's internal controls. The Commission, therefore, distinguishes between the COSO framework as a definition of what constitutes an effective system of internal control and guidance on how to evaluate internal control over financial reporting for purposes of the SEC rules.

Internal Control over Financial Reporting

Although Section 404 did not define the term internal control over financial reporting, the regulators have defined it as process designed by, or under the supervision of, the company's principal executive and financial officers, and effected by the company's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with GAAP 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 company assets;
- Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with GAAP, and that receipts and expenditures of the company are being made only in accordance with management authorizations; and
- Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements. (AS 5, ¶A5.)

It should be noted that the outside auditor's procedures as part of either the audit of internal controls or the audit of the financial statements are not part of a company's internal control over financial reporting. It must also be recognized that internal control over financial reporting has inherent limitations. It is a process involving human diligence and compliance. It is also subject to lapses in judgment and breakdowns resulting from human failures.

Internal control over financial reporting also can be circumvented by collusion or improper management override. Because of such limitations, there is a risk that material misstatements will not be prevented or detected on a timely basis by internal control over financial reporting. However, these inherent limitations are known features of the financial reporting process. Therefore, it is possible to design into the process safeguards to reduce, though not eliminate, this risk. (AS 5, ¶A5.)

SEC Management Guidance: Broad Principles

The SEC's management guidance is organized around two broad principles. The first principle is that management should evaluate the design of the controls that it has implemented to determine whether they adequately address the risk that a material misstatement in the financial statements would not be prevented or detected in a timely manner. The guidance describes a top-down, risk-based approach to this principle, including the role of entity-level controls in assessing financial reporting risks and the adequacy of controls. The guidance promotes efficiency by allowing

management to focus on those controls that are needed to adequately address the risk of a material misstatement in the financial statements.

The guidance does not require the identification of every control in a process or the documentation of the business processes impacting internal controls. Rather, management should focus its evaluation process and the documentation supporting the assessment on those controls that it believes adequately address the risk of a material misstatement in the financial statements. For example, if management determines that the risks for a particular financial reporting element are adequately addressed by an entity-level control, no further evaluation of other controls is required.

The second principle is that management's evaluation of evidence about the operation of its controls should be based on its assessment of risk. The guidance provides an approach for making risk-based judgments about the evidence needed for the evaluation. This allows management to align the nature and extent of its evaluation procedures with those areas of financial reporting that pose the greatest risks to reliable financial reporting, that is whether the financial statements are materially accurate. As a result, management may be able to use more efficient approaches to gathering evidence, such as self-assessments, in low-risk areas and perform more extensive testing in high-risk areas.

By following these two principles, emphasized the SEC, companies of all sizes and complexities will be able to implement the internal control rules effectively and efficiently. As smaller public companies have less complex internal control systems than larger public companies, this top-down, risk-based approach enables smaller public companies in particular to scale and tailor their evaluation methods and procedures to fit their own facts and circumstances. Indeed, the SEC encourages smaller public companies to take advantage of the flexibility and scalability of this approach to conduct an efficient evaluation of internal control over financial reporting.

While a company's individual facts and circumstances should be considered in determining whether a company is a smaller public company, a company's market capitalization and annual revenues are useful indicators of its size and complexity. In light of the Advisory Committee Final Report and the SEC rules defining "accelerated filers" and "large accelerated filers," companies with a market capitalization of approximately $700 million or less, with reported annual revenues of approximately $250 million or less, are presumed to be smaller companies, with the smallest of these companies, with a market capitalization of approximately $75 million or less, described as microcaps.

Evaluation Process

The information management gathers and analyzes from its evaluation process serves as the basis for its assessment on the effectiveness of its internal controls. The extent of effort required for a reasonable evaluation process will largely depend on the company's existing policies,

procedures and practices. For example, in some situations management may determine that its existing activities, which may be undertaken for other reasons, provide information that is relevant to the assessment. In other situations, management may have to implement additional procedures to gather and analyze the information needed to provide a reasonable basis for its annual assessment.

The guidance does not explain how management should design its internal controls to comply with the control framework it has chosen. Similarly, in order to allow appropriate flexibility, the guidance does not provide a checklist of steps management should perform in completing its evaluation. Rather, it describes a top-down, risk-based approach allowing for the exercise of significant judgment so that management can design and conduct an evaluation that is tailored to its company's individual circumstances.

Under the guidance, management can align the nature and extent of its evaluation procedures with those areas of financial reporting that pose the highest risks to reliable financial reporting, that is, whether the financial statements are materially accurate. As a result, management may be able to use more efficient approaches to gathering evidence, such as self-assessments, in low-risk areas and perform more extensive testing in high-risk areas. By following these two principles, the SEC believes that companies of all sizes and complexities will be able to implement the internal control mandate effectively and efficiently.

While expressing support for the principles-based approach embodied in the guidance, some commenters requested that additional guidance and illustrative examples be provided in areas such as the identification of controls that address financial reporting risks, including IT general controls; the assessment of risk; and how risk impacts the nature, timing and extent of evidence needed to support the assessment. However, the SEC decided that additional specificity and examples in the areas requested would negatively establish a bright line or one-size fits all evaluation approach, thereby negating the scaled, principles-based approach the SEC wants to achieve.

Overly prescriptive rules can lead to inefficiencies, and the Commission wants to avoid ending up with evaluations more concerned with form than substance and which are inefficient to implement or ineffective in detecting material weaknesses. Thus, the guidance takes the view that effective and efficient evaluations require management to make reasonable judgments reflecting each company's individual facts and circumstances.

The guidance indicates that management should implement and conduct an evaluation that is sufficient to provide it with a reasonable basis for its annual assessment. Management should use its own experience and informed judgment in designing an evaluation process that aligns with the operations, financial reporting risks and processes of the company.

The guidance comports with the COSO framework, which cautions that, because facts and circumstances vary between entities and industries, evaluation methodologies and documentation

will also vary. Accordingly, entities may use different evaluation tools, or use other methodologies utilizing different evaluative techniques.

If the evaluation process identifies material weaknesses that exist as of the fiscal year-end, those weaknesses must be disclosed in management's annual report with a statement that the internal controls are ineffective. If the evaluation identifies no internal control deficiencies that constitute a material weakness, management assesses the internal controls as effective.

Entity-Level Controls

Entity-level controls (commonly called company-level controls), such as controls within the control environment, have a pervasive and important effect on the company's internal control system, and an indirect effect on the likelihood that a misstatement will be prevented or detected on a timely basis. Further, the guidance clarifies that some entity-level controls may be designed to identify possible breakdowns in lower-level controls, but not in a manner that would, by themselves, adequately address financial reporting risks.

In these cases, management would identify the additional controls needed to adequately address financial reporting risks, such as those that operate at the transaction or account balance level. However, management would consider both the entity-level and transaction level in designing the nature and extent of the evaluation procedures, including those for transaction level control.

The SEC has also clarified that those controls management identifies should include the entity-level and pervasive elements of its internal controls that are necessary for reliable financial reporting. This rubric emphasizes that management's evaluation of internal controls should consider the control environment, and other entity level activities, that are necessary to have a system of internal control that is effective at providing reasonable assurance regarding the reliability of financial reporting. In addition to control environment, other entity-level controls include controls related to risk assessment, centralized processing, period-end financial process, and management override

Ongoing Monitoring

The SEC has provided management guidance regarding ongoing monitoring activities, including self-assessments, and direct testing. Evidence obtained from each of the activities can vary. Under the guidance, management's assessment can be supported by information it obtains from normal monitoring activities, which will often be built-in to the daily responsibilities of employees involved in its processes, rather than from consultants hired for testing purposes. The guidance contains a discussion of how management should consider the objectivity of the

individuals performing the activities when determining the evidence obtained from each of the activities.

As part of this discussion, the SEC clarified that, when evaluating the objectivity of personnel, management is not required to make an absolute conclusion regarding objectivity, but rather should recognize that personnel will have varying degrees of objectivity based on their job function, their relationship to the subject matter, and their status within the organization. Management should consider the risk to reliable financial reporting when determining whether the objectivity of the personnel involved in the monitoring activities results in sufficient evidence.

Fraud Risk

Commenters suggested that further guidance in the area of fraudulent financial reporting would improve the proposal. Thus, the SEC provides general direction to assess the risk of fraud and to focus evaluation procedures on controls that address such risks. The final guidance was enhanced by explaining that the risk of fraudulent financial reporting will exist in virtually all companies. Rigorous evaluations require management to recognize that the existence of a fraud risk does not mean that fraud has occurred. Likewise, and importantly, it should not take an incident of fraudulent financial reporting to recognize the existence of fraud risk.

Further, the guidance clarifies that the risk of management override, particularly in the period-end financial reporting process, is something that virtually every company needs to consider. Effective control systems ought to take steps to manage this risk, and the SEC believes that companies of all sizes, including smaller companies, can do so.

Paths to Compliance

The SEC's internal control rules have been amended to state that, while there are many different ways to conduct an evaluation of the effectiveness of internal control over financial reporting, an evaluation conducted in accordance with the interpretive guidance will satisfy the rules. An important point here is that the SEC understands that many of the larger public companies already complying with Section 404 have established a compliant evaluation process that may differ from the approach described in the interpretive guidance. That is okay, said Corporation Finance Director John White, since there is no requirement for these companies to alter their procedures from the last three years to align them with the new interpretive guidance, unless they choose to do so

The Commission's management guidance should reduce uncertainty about what constitutes a reasonable approach to management's evaluation while maintaining flexibility for companies that have already developed their own assessment procedures and tools that serve the company and its investors well. Companies will be able to continue using their existing procedures if they choose, provided of course that those meet the standards of Section 404 and the rules.

The Commission also approved rule amendments providing that a company that performs an evaluation of internal control in accordance with the interpretive guidance satisfies the annual evaluation required by Exchange Act Rules 13a-15 and 15d-15. The amendments are similar to a non-exclusive safe-harbor in that they would not require management to comply with the evaluation requirement in a particular manner (i.e., by following the interpretive guidance), but would provide certainty to management choosing to follow the guidance that management has satisfied its obligation to conduct an evaluation in an appropriate manner.

All public companies, especially smaller companies, that choose to follow the guidance would be afforded considerable flexibility to scale and tailor their evaluation methods and procedures to fit their own facts and circumstances. Management would have the comfort of a safe harbor that an evaluation that complies with the interpretive guidance is one way to satisfy the evaluation required by SEC rules, thus reducing any second-guessing as to whether management's process was adequate.

Managers may choose to rely on the interpretive guidance, as an alternative to what is provided in existing auditing standards or elsewhere, for two key reasons. First, SEC rules now give managers who follow the interpretive guidance comfort that they have conducted a sufficient internal controls evaluation.

Second, elimination of the auditor's opinion on management's assessment of internal controls in the auditor's attestation report should significantly lessen, if not eliminate, the pressures that managers have felt to look to auditing standards for guidance in performing those evaluations. (See discussion below.) The auditor will now express only a single opinion on the effectiveness of the company's internal controls in its attestation report rather than expressing separate opinions directly on the effectiveness of the company's internal controls and on management's assessment.

Previously, in the absence of specific guidance, managers had relied on AS2 because they were under pressure to meet the expectations of the auditors who were charged with attesting to the effectiveness of the company's internal controls and management's annual assessment of internal controls. AS2 had become an essentially de facto standard for management.

Since reliable financial statements must be materially accurate, an overall objective of internal control over financial reporting is to foster the preparation of reliable financial statements. Therefore, the central purpose of management's evaluation of the effectiveness of the company's internal controls is to assess whether there is a reasonable possibility of a material misstatement in the financial statements not being prevented or detected on a timely basis by the company's

internal controls. In turn, management's assessment is based on whether any material weaknesses exist as of the end of the fiscal year. (See below discussion on material weakness.)

Reasonable Assurance

Management must assess as of the fiscal year-end whether the company's internal control over financial reporting is effective in providing reasonable assurance regarding the reliability of financial reporting. Management is not required by Section 404 to assess other internal controls, such as controls solely implemented to meet a company's operational objectives.

Further, reasonable assurance does not mean absolute assurance since internal controls cannot prevent or detect all misstatements, whether unintentional errors or fraud. Rather, the reasonable assurance referred to in the Commission's implementing rules relates to similar language in the Foreign Corrupt Practices Act, specifically Exchange Act Section 13(b)(7), which defines "reasonable assurance" and "reasonable detail" as such level of detail and degree of assurance as could satisfy prudent officials in the conduct of their own affairs.

The Commission has long held that reasonableness is not an absolute standard of exactitude for corporate records. In addition, the Commission recognizes that while reasonableness is an objective standard, there is a range of judgments that an issuer might make as to what is reasonable in implementing Section 404 and the Commission's rules. Thus, the terms reasonable, reasonably and reasonableness in the context of Section 404 implementation do not imply a single conclusion or methodology, but encompass the full range of appropriate potential conduct, conclusions or methodologies on which an issuer may reasonably base its decisions.

The conference committee report on amendments to the FCPA also noted that the standard "does not connote an unrealistic degree of exactitude or precision. The concept of reasonableness of necessity contemplates the weighing of a number of relevant factors, including the costs of compliance." Cong. Rec. H2116 (daily ed. April 20, 1988).

Audit Committees

Because management is responsible for maintaining effective internal control over financial reporting, the interpretive guidance does not specifically address the role of the board of directors or audit committee in a company's evaluation and assessment of internal controls. However, the SEC expects a board of directors or audit committee, as part of its oversight duties for the company's financial reporting, to be knowledgeable and informed about the evaluation process and management's assessment, as necessary in the circumstances. It may also be a good practice if management documentation supporting its assessments be separately maintained in order to assist the audit committee in exercising its oversight of corporate financial reporting.

Auditor Need No Longer Evaluate Management's Process

Working in tandem, the SEC and PCAOB eliminated the need for the outside auditor to evaluate and report on management's annual internal control evaluation process. Now, under AS 5 and the SEC's revised rules, the auditor will express only one opinion; and that will be an opinion on the effectiveness of the company's internal control over financial reporting.

Two Regulation S-X provisions pertaining to the auditor's attestation report on internal control over financial reporting were clarified so that, going forward, the auditor will be required to express only one opinion directly on the effectiveness of internal control over financial reporting in its audit report. Under prior rules, the auditor had to express two separate opinions; one on effectiveness and another on management's assessment. This revision clearly conveys that the auditor is not evaluating management's evaluation process but is opining directly on the company's internal controls.

The SEC rule changes allowed the Board to remove the requirement that the auditor evaluate management's process. Since the auditor will still have to test controls directly in some cases to determine if they are effective, the Board believes that the auditor can perform an effective audit of internal control without conducting an evaluation of the adequacy of management's evaluation process.

Further, although the removal of the evaluation requirement should eliminate unnecessary work, noted the Board, the quality of management's process is inherently linked to the amount of work the auditor will need to do. For example, the extent of the auditor's ability to use the work of others will depend on the quality of the company's annual evaluation process and its ongoing monitoring activities, as well as on the competence and objectivity of those performing the work. (Proposing Release No. 2006-007.)

Material Weakness

The definition of "material weakness" is a central feature of the reforms because management's assessment of the company's internal controls is based on whether any material weaknesses exist. Similarly, the objective of an audit of internal control is to obtain reasonable assurance as to whether material weaknesses exist. The term's importance is evident from the rule that management is not permitted to conclude that the company's internal controls are effective if there are one or more material weaknesses. Similarly, under AS 5, the outside auditor must express an adverse opinion on the company's internal controls if there is a material weakness. (AS 5, ¶90.)

Note that a material weakness in internal control over financial reporting may exist even when financial statements are not materially misstated.

Initially, the SEC did not have its own definition of material weakness. Rather, the SEC staff earlier said that it would apply the PCAOB's definition of material weakness when applying Commission rules. Previously, Auditing Standard No. 2 defined material weakness as a significant deficiency, or combination of significant deficiencies, resulting in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. Acting on complaints that this definition was confusing and made it difficult to assess the severity of deficiencies, the Board revised the definition in Auditing Standard No. 5.

At the same time, the SEC codified the definition of the term material weakness. SEC rules, and AS 5, define a material weakness as a deficiency, or a combination of deficiencies, in internal control over financial reporting 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.

Reasonable Possibility Standard

Note that the regulators replaced the standard "more than a remote likelihood" with "reasonable possibility" based on their belief that companies and auditors were evaluating the likelihood of a misstatement at a much lower threshold than was intended. The new standard should, in the Board's view, result in the identification of the most important material weaknesses.

Admittedly, the evaluation of deficiencies is inherently one of the most difficult aspects of an audit of internal control. Given the individual characteristics of each company and each deficiency, any method for evaluating deficiencies demands a high degree of professional judgment.

To the extent the previous use of the term "more than remote" in the definition of material weakness resulted in auditors and issuers evaluating the likelihood that a misstatement in the financials would not be prevented at a more stringent level than originally intended, the Board believes that the new definition should significantly improve the evaluation of deficiencies such that material weaknesses, when identified, are actually the most important deficiencies. (Proposing Release No. 2006-017.)

While agreeing that the current "more than remote likelihood" is too low a probability standard, the American Bar Association said earlier in a comment letter that inserting reasonable possibility would not change the probability standard. Accountants have interpreted the terms remote, reasonably possible and probable, as used in FASB Standard No. 5, Accounting for Contingencies, as levels of probability that are contiguous, noted the ABA..

The auditors interpret it as, once an event is more probable than remote, it is reasonably possible. This interpretation of reasonably possible leads to events being reasonably possible at a

probability level of substantially less than 50%. In fact, said the ABA, some accountants take the position that reasonable possibility is triggered at a probability level of as low as 25%. The bar groups believe that such a level of probability is too low for this purpose.

One commenter recommends that the adoption of a "reasonably likely" standard" to replace "more than a remote likelihood." The commenter found it difficult to see how replacing the term "more than remote likelihood" with its synonym under SFAS No. 5, "reasonable possibility," will have a meaningful impact on issuer or auditor behavior. The commenter pointed out that the "reasonably likely" threshold is used by the SEC in connection with MD&A disclosure and is well understood by both issuers and auditors. Because it is meaningfully higher than the "more than remote" standard, it reasoned, a "reasonably likely" threshold will have a better chance of focusing the evaluation and audit on the deficiencies that are of greatest concern to investors.

Severity of Deficiencies

Obviously, a key determination in finding a material weakness is evaluating identified deficiencies. Under AS 5, auditors must evaluate the severity of each control deficiency that comes to their attention to determine whether the deficiencies are material weaknesses as of the date of management's assessment. However, auditors are not required to search for deficiencies that are less severe than a material weakness. (AS 5, ¶62.)

The severity of a deficiency depends on whether there is a reasonable possibility that the controls will fail to prevent a misstatement of an account balance or disclosure and the magnitude of the potential misstatement resulting from the deficiency. The severity of a deficiency does not depend on whether a misstatement has actually occurred but rather on whether there is a reasonable possibility that the controls will fail to prevent a misstatement. (AS 5, ¶s 63 and 64.)

Risk factors affect whether there is a reasonable possibility that a deficiency will result in a misstatement, including,

- The nature of the accounts and disclosures involved;
- The susceptibility of the related asset or liability to loss or fraud;
- The subjectivity or complexity of judgment required to determine the amount involved;
- The interaction of the control with other controls, including whether they are interdependent or redundant;
- The interaction of the deficiencies; and
- The possible future consequences of the deficiency.

Also, the evaluation of whether a control deficiency presents a reasonable possibility of misstatement can be made without quantifying the probability of occurrence as a specific

percentage or range. Further, multiple control deficiencies affecting the same financial statement account balance or disclosure increase the likelihood of misstatement and may, in combination, constitute a material weakness, even though such deficiencies may individually be less severe. Therefore, the auditor should determine whether individual control deficiencies that affect the same significant account or disclosure, relevant assertion, or component of internal control collectively result in a material weakness.

The Board has provided a non-exclusive list of factors affecting the magnitude of the misstatement that might result from a control deficiency:

- The financial statement amounts or total of transactions exposed to the deficiency; and
- The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred.

In evaluating the magnitude of the potential misstatement, the maximum amount that an account balance or total of transactions can be overstated is generally the recorded amount, while understatements could be larger. Also, in many cases, the probability of a small misstatement will be greater than the probability of a large misstatement.

Further, AS 5 says that the auditor should evaluate the effect of compensating controls when determining whether a control deficiency is a material weakness. To have a mitigating effect, the compensating control should operate at a level of precision that would prevent or detect a misstatement that could be material. (AS 5, ¶68.)

Material Weakness Indicators

AS 5 also contains a list of indicators of material weaknesses in internal controls:

- Identification of fraud on the part of senior management;
- Restatement of financial statements reflecting the correction of a misstatement;
- Identification by the auditor of a misstatement in circumstances indicating that it would not have been detected by the company's internal controls; and
- Ineffective oversight of the company's external financial reporting and internal controls by the audit committee. (AS 5, ¶69.)

The list of indicators of a material weakness is not exhaustive and should not be used as a checklist. The presence of one of the indicators does not mandate a conclusion that a material weakness exists. At the same time, a deficiency that is not a listed indicator may be a material weakness.

The Board noted that the identification of one of these indicators should bias auditors toward a conclusion that a material weakness exists in the internal controls, but does not require them to reach that conclusion. Instead, the auditor may determine that these circumstances do not rise to the level of a material weakness. In order not to interfere with the auditor's judgment in making these evaluations, the Board removed from AS 5 the previous requirement that these indicators must at least be considered deficiencies. (Proposing Release No. 2006-007.)

When evaluating the severity of a deficiency, the auditor should determine the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with GAAP. If the auditor determines that a deficiency might prevent prudent officials in the conduct of their own affairs from concluding that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with GAAP, then the auditor should treat the deficiency as an indicator of a material weakness. (AS 5, ¶70.)

For purposes of the material weakness indicator of senior management identifying fraud, AS 5 defines "senior management" as the principal executive and financial officers signing the company's Sarbanes-Oxley 302 certifications, as well as any other members of senior management who play a significant role in the company's financial reporting process.

Audit Committee Pre-Approval of Non-Audit Services

The PCAOB also adopted a rule requiring the auditor to obtain pre-approval from the audit committee for the performance of any non-audit internal control services. The Sarbanes-Oxley Act requires audit committee pre-approval of all non-audit services that the auditor proposes to perform for the client company.

Rule 3525 implements this pre-approval requirement by requiring auditors to take certain steps as part of seeking audit committee pre-approval of internal control related non-audit services. These steps are intended to ensure that audit committees are provided the information they need to make an informed decision on how the performance of internal control-related services may affect the auditor's independence.

Specifically, the auditor seeking pre-approval to perform non-audit internal control services would have to:

- Describe, in writing, to the audit committee the scope of the proposed service;
- Discuss with the audit committee the potential effects of the proposed service on the firm's independence; and

- Document the substance of the firm's discussion with the audit committee.

These requirements parallel the auditor's responsibility in seeking audit committee pre-approval to perform tax services for an audit client under PCAOB Rule 3524 and are codified, like that rule, as part of the Board's rules on ethics and independence.

Consistent with the tax service pre-approval rule, Rule 3525 does not specify that the pre-approval must be specific. Instead, the rule is neutral as to whether an audit committee pre-approves a non-audit service on an ad hoc basis or on the basis of policies and procedures.

Many companies have adopted policies providing for pre-approval in annual audit committee meetings. And the Board understands that such an annual planning process can include as robust a presentation to the audit committee as a case-by-case pre-approval process. Thus, Rule 3525 is flexible enough to accommodate either system and encourages auditors and audit committees to develop systems tailored to the needs and attributes of the company.

A Note to Rule 3525 explains the general standard of auditor independence, and that application of this standard is guided by several principles, including whether auditors assume a management role or audit their own work. The Note further specifies, as an example of the standard's application, that an auditor would not be independent if management had delegated its duty for internal control to the auditor or if the auditor had designed or implemented the audit client's internal controls.

Auditing Standard No. 5: Background

AS 5 is a new principles-based audit standard designed to assure that the auditor, at every step of the audit process, can take into account the individual facts and circumstances of a particular company. Depending on the nature of the audit client and its control environment, the auditor may utilize different combinations of procedures. A principles-based standard gives the auditor room to exercise judgment in determining what specific procedures are required in order to obtain sufficient evidence.

According to PCAOB Chair Olson, the Board made an effort in developing AS 5 to provide appropriate room for judgment, which is underscored by the top-down approach to the audit process. At the same time, the standard provides a sufficient framework to assure that an audit performed in accordance with its requirements will be effective. In addition, a principles-based standard has the flexibility to be scaled for an audit of a global company spanning several continents or a very small company.

The Board has promised that its standards and inspections staff will work closely with audit firms on effective implementation of AS 5. For example, the inspection program will be adjusted to be consistent with the new standard. Moreover, the new standard's principles-based approach

will provide room for companies and auditors to evolve, and the Board will work closely with its inspections staff to assure that it remains informed and allows for innovation

The organizing principle of AS 5 is the top-down concept, under which the auditor focuses on entity-level controls and works downward, planning the audit so that testing of lower-level controls is influenced by the strengths and weaknesses of those above. But the Board emphasizes that the approach is more one of reasoning than work sequence, and that the auditor needs to use judgment, not follow a roadmap.

The final standard underscores that walkthroughs, the process by which the auditor traces a transaction from cradle to grave through the company's reporting system, are not an end in themselves, but rather a means to attaining an understanding of likely sources of misstatement. This change reduces the risk that walkthroughs will become just another step that must be performed without much understanding as to why the work is being done.

The new standard requires the auditor to communicate to the audit committee control deficiencies identified during the audit that are less severe than material weaknesses, but important enough to merit the attention of those responsible for the company's financial reporting. This replaces the approach in AS No. 2, which relied on the auditor's ability to make difficult determinations about the application of abstract phrases like "more than remote" and "more than inconsequential" to deficiencies. The standard puts the emphasis on the auditor's professional judgment and expertise.

Similarly, the final standard rephrases the discussion of circumstances that are indicators of material weaknesses. The new version should increase the likelihood that material weaknesses will serve as an early warning system, rather than merely as after-the-fact acknowledgments that something has gone wrong.

The final standard affords the auditor greater latitude to use the results of testing performed by the company's internal audit or other staff. However, that goal is accomplished by referring the auditor to the familiar criteria on use of the work of others, rather than by creating a new standard with new criteria.

According to Board Member Goelzer, AS 5 will preserve the benefits of internal control auditing, while at the same time focus auditor energy and resources on the mountains, rather than the molehills, of internal control. The framework can be applied to smaller, less complex companies in a way that matches costs and benefits.

AS 5 does allow scaling of the internal control audit to accommodate smaller companies, but it does not exempt them. As put by Member Gradison: Do investors deserve any less assurance over the accuracy and reliability of audited financial reports because a public company is small. The statutory mission of the PCAOB is to protect investors, he said, and no distinctions are made with respect to company size.

In addition, it is significant that throughout the long and open process of crafting this new auditing standard to replace AS 2, there has been little or no sentiment from the investor community for carving out exceptions or safe harbors for small public companies simply because they happen to be small. But there was broad and deep support in the investor community for a scalable internal-control auditing standard that takes into account the complexity as well as the size of public companies. AS 5 delivers such scalability, not just for small companies but also for divisions of larger companies.

Audit committees will have a role under AS 5. Sarbanes-Oxley makes fundamental changes that empower audit committees by requiring that they, not management, hire and oversee the external, independent auditor. This means, necessarily and by design, that audit committees are intended to function as traffic cops when it comes to disagreements between management and the auditor over GAAP and over internal controls.

A good example of this new governance model has to do with significant deficiencies. These are defects in internal controls that are less severe than material weaknesses yet are serious enough to merit attention by those in charge of the company's financial reporting, which is, first and foremost, the company's audit committee. Although auditors are, under AS 5, only required to seek out material weaknesses, they are nevertheless required to communicate deficiencies of which they are aware, in certain instances to management and in others to the audit committee. By focusing the auditor on the identification of material weaknesses rather than on significant deficiencies, AS 5 has been carefully and deliberately crafted so as not to cause auditors to do more work than necessary.

Under the Commission's management guidance and the Board's AS 5, both management and the auditor will be required to report to the audit committee any significant deficiencies (as well as all material weaknesses) of which they are aware. Because both the SEC's guidance and AS 5 are principles-based, it is entirely possible that management and the auditors will, at times, disagree over what is, or is not, a significant deficiency or material weakness. Member Gradison believes that having the communication of significant deficiencies come from two separate sources will enhance the ability of audit committees to carry out their clear statutory responsibilities to investors.

According to Board Member Neimeier, the ultimate success of a principles-based standard depends on how it is implemented in practice. Thus, obtaining the benefits of AS 5 will require faithful application of the principles in the standard. This will also require consistent and balanced oversight of firms' implementation, and concern for more than just reducing costs.

In the view of Board Member Gillan, AS 5 lays out clear objectives that auditors must meet and for which they will be held accountable. Most importantly, these objectives rationally relate to the purpose of the internal control audit, that is, to provide investors with the independent auditor's reasoned and reasonable judgment as to whether a company's controls are structured so that financial reporting is likely to be materially accurate. Secondarily, auditors should be able to

meet the objectives of this standard in a way that does not require the expenditure of unnecessary resources.

In adopting AS 5, the Board was mindful of the inherent differences in the roles of management and the auditor. Management's daily involvement with its internal control system provides it with knowledge that may influence its judgments about how best to evaluate internal control and the sufficiency of the evidence it needs for its annual assessment. Management also should be able to rely on self-assessment and, more generally, the monitoring component of internal control, provided the monitoring component is properly designed and operates effectively. On the other hand, the auditor is required to provide an independent opinion on the effectiveness of the company's internal controls.

The auditor does not have the familiarity with the company's controls that management has and does not interact with these controls with the same frequency as management. Therefore, the auditor cannot obtain sufficient evidence to support an opinion on the effectiveness of internal control based solely on interaction with the company's controls. Rather, the auditor needs to perform procedures such as inquiry, observation, and inspection of documents, or walkthroughs, which consist of a combination of those procedures, in order to fully understand and identify the likely sources of potential misstatements, while management might be aware of those risk areas on an ongoing basis.

Fraud Controls

The discussion of fraud risk and antifraud controls has been moved closer to the beginning of the standard and made part of planning the audit to emphasize to auditors the relative importance of these matters in assessing risk throughout the top-down approach. Every company has an inherent level of fraud risk, and auditors must be cognizant of that risk in each audit. The prominence that AS 5 gives to fraud risk and anti-fraud controls emphasizes to the outside auditors the importance of assessing fraud risk throughout the audit process.

AS 5 requires auditors to consider the results of their fraud risk assessment when planning and performing the audit. The Board believes that incorporating the fraud risk assessment, which is required in the financial statement audit, into the planning process for the audit of internal controls will promote audit quality as well as better integration.

While internal controls cannot provide absolute assurance that fraud will be prevented or detected, said the Board, these controls should help to reduce instances of fraud, and, therefore, a concerted focus on fraud controls in the internal control audit should enhance investor protection. Second, management fraud has also been identified in the final standard as an area of higher risk; accordingly, auditors should focus more of their attention on this area.

Finally, the standard lists the types of controls that might address fraud risk:

- Controls over significant, unusual transactions;
- Controls over journal entries and adjustments made in the period-end financial reporting process;
- Controls over related party transactions;
- Controls related to significant management estimates; and
- Controls that mitigate incentives for, and pressures on, management to falsify financial results. (AS 5, ¶14.)

Walkthroughs

In an audit of internal control, performing a walkthrough is an effective way for the auditor to gain an understanding of the company and its controls, determine what has changed within the company and its internal control from year to year, and evaluate the design of internal control in a disciplined manner. Walkthroughs can also help auditors understand likely sources of potential misstatements and help in selecting controls to test.

AS 5 articulates the principle that performance of a walkthrough might provide sufficient evidence of operating effectiveness, depending on the risk associated with the control being tested, the specific procedures performed as part of the walkthroughs, and the results of the procedures performed. Based on the experience of the past two years, the Board believes that walkthroughs are essential to every audit of internal control but that the number required can be reduced without negatively affecting audit quality.

Essentially, walkthroughs require the auditor to get out of the audit room and interact with those responsible for internal control from day to day. They also provide the auditor with the opportunity to learn about the everyday activities of the company, which may not be reflected in any document that the auditor reviews.

While a walkthrough will frequently be the best way of attaining these goals, noted the Board, the auditor's focus should be on the objectives, not on the mechanics of the walkthrough. And in some cases, other procedures may be equal or more effective means of a achieving them.

A sound walkthrough envisions the auditor following the transaction from origination through the company's processes, including information systems, until it is reflected in the company's financial records, using the same documents and IT that company personnel use. Walkthrough procedures usually include a combination of inquiry, observation, inspection and re-performance of controls. (AS 5, ¶37.)

In performing a walkthrough, at the points at which important processing procedures occur, the auditor questions the company's personnel about their understanding of what is required by the procedures and controls. These probing questions, combined with the other walkthrough procedures, allow the auditor to gain a sufficient understanding of the process and to be able to identify important points at which a necessary control is missing or not designed effectively. Additionally, probing beyond the single transaction used as the basis for the walkthrough allows the auditor to understand the different types of significant transactions handled by the process. (AS 5, ¶38.)

AS 5 lists a number of objectives that a walkthrough can help attain, including identifying management controls to address potential misstatements or detect or prevent misstatements. Another objective is to understand the flow of transactions related to relevant assertions. (AS 5, ¶34.)

Using Work of Others

AS 5 allows the outside auditor to use the work of others to obtain evidence about the design and operating effectiveness of controls. Also, recognizing that issuers might employ personnel other than internal auditors to perform activities relevant to management's assessment of internal controls, the standard allows the auditor to use the work of company personnel other than internal auditors, as well as third parties working under the direction of management or the audit committee.

Importantly, AS 5 also eliminates the principal evidence provision formerly contained in AS2. The principal evidence provision required that the auditor's own work be the principal evidence for the auditor's opinion. This provision had limited the use of the work of others, particularly in lower-risk areas.

Consistent with the standard's risk-based approach, the extent to which auditors may use the work of others depends on the risk associated with the control being tested. As the risk decreases, so does the need for auditors to perform the work themselves. Conversely, in higher risk areas, such as controls addressing fraud risks, using the work of others would be limited if such work could be used at all. Similarly, the impact of the work of others on the auditor's work also depends on the relationship between the risk and the competence and objectivity of those who performed the work. As the risk decreases, the necessary level of competence and objectivity decreases as well.

Note that, because of the degree of judgment required, auditors must either perform the procedures to understand potential sources of misstatements themselves or supervise the work of others who provide direct assistance to the auditors. (AS 5, ¶35.)

Further, in determining the locations or business units at which to perform tests of controls, the outside auditors may take into account work performed by others on behalf of management. For example, if the internal auditors plan relevant audit work at various locations, the independent auditors may coordinate work with the internal auditors and reduce the number of locations or business units at which they would otherwise need to perform auditing procedures. (AS 5, ¶B12.)

Communicating Deficiencies

AS 5 requires auditors to report, in writing, to management and the audit committee all identified material weaknesses before issuing their report on the internal controls. (AS 5, ¶78.) The standard also requires auditors to provide relevant information about important control deficiencies, even those less severe than a material weakness, to management and to the audit committee. Specifically, the auditor must communicate any identified significant deficiencies to the audit committee. In order to emphasize that the auditor need not scope the audit to identify all significant deficiencies, however, the Board placed these provisions in the section of the standard describing communications requirements. (AS 5, ¶80.)

AS 5 also requires the auditor to communicate, in writing, to management, all deficiencies in internal control identified during the audit and inform the audit committee when such a communication has been made. (AS 5, ¶79.) The auditor must also, when applicable, inform the board of directors of the auditor's conclusion that the audit committee's oversight is ineffective. (AS 5, ¶81.)

But because the audit of internal controls does not provide auditors with assurance that they have identified all deficiencies less severe than a material weakness, they should not issue a report stating that no such deficiencies were issued during the audit. (AS 5, ¶83.)

Scaling the Audit

Scaling the audit is a natural extension of the risk-based approach and applies to all companies, not just small companies. In that spirit, although scaling is often thought of in terms of smaller companies, the Board believes that the audit should be scaled to a less complex company or to a unit of a larger company. Scalability is also closely tied to the principles-based approach embodied in AS 5.

Thus, the Board incorporated a discussion of scaling concepts throughout the standard. Specifically, notes to relevant paragraphs describe how to tailor the audit to the particular circumstances of a smaller, less complex company or unit. The Board also lists attributes of smaller, less complex companies and acknowledges that, even within larger companies, some business units or processes may be less complex than others.

Discussion of these attributes has been incorporated in the section on the auditor's planning procedures in the standard. (AS 5, ¶9.) In addition, the provisions on scalability in the standard will form the basis for guidance on auditing internal control in smaller companies to be issued this year.

By incorporating the discussion of scaling concepts throughout the standard, rather than in one specific section, said PCAOB Chair Olson, the Board strengthened the impact of scaling. That is, the top-down, risk-based approach is fundamentally designed so that an auditor will tailor the audit to the specific profile of a company.

Smaller companies have neither been exempted from Section 404 nor been accorded a version of "404 lite." That said, the Board recognizes that complying with Section 404 has posed challenges for smaller public companies. In considering how to minimize the costs of the audit of internal control while preserving its benefits, the Board also realizes that smaller companies often present different financial reporting risks than larger and more complex ones and that their internal control systems often appropriately address those risks in different ways. Thus, AS 5 recognizes that a company's size and complexity are important and that the procedures an auditor should perform depend on where along the size and complexity continuum a company falls.

The Board expects that the broad changes in the proposals that are designed to eliminate unnecessary audit work for all companies will particularly affect smaller company audits. In general, the reliance on principles rather than detailed instruction would require auditors to consider each company's unique facts and circumstances before determining how to apply the standard.

Specific changes, which include focusing the auditor on the most important controls and using risk to determine the necessary evidence, and thus the auditor's effort, should together make the audit more scalable for any company. Under the standard, the auditor can use strong entity-level controls and financial statement audit procedures to reduce the level of testing for smaller companies. (Proposing Release No. 2006-007.)

Integrating Internal Control and Financial Statement Audits

The audit of internal control over financial reporting should be integrated with the audit of the financial statements. The objectives of the audits are not identical, however, and the auditor must plan and perform the work to achieve the objectives of both audits. (AS 5, ¶6.)

Moreover, in an integrated audit of internal controls and the financial statements, auditors should design their testing of controls to accomplish the objectives of both audits simultaneously:

- To obtain sufficient evidence to support the auditor's opinion on internal controls at year end; and

- To obtain enough evidence to support the auditor's control risk assessments for purposes of the audit of financial statements.

Planning the Audit

AS 5 requires that the audit be properly planned and supervised. When planning an integrated audit, the auditor should evaluate whether the following matters are important to the company's financial statements and internal controls and, if so, how they will affect the auditor's procedures:

- Knowledge of the company's internal controls obtained during other engagements performed by the auditor;
- Matters affecting the industry in which the company operates;
- Matters relating to the company's business and capital structure;
- The extent of any recent changes in the company's internal controls;
- The auditor's preliminary judgments about materiality, risk, and other factors relating to the determination of material weaknesses;
- Control deficiencies previously communicated to the audit committee or management;
- Legal or regulatory matters of which the company is aware;
- The type and extent of available evidence related to the effectiveness of the company's internal controls;
- Preliminary judgments about the effectiveness of internal controls;
- Public information about the company relevant to the evaluation of the likelihood of material financial statement misstatements and the effectiveness of the internal controls;
- Knowledge about risks related to the company evaluated as part of the auditor's client acceptance and retention evaluation; and
- The relative complexity of the company's operations.

In a note related to scaling the audit, the Board said that many smaller companies have less complex operations, and some larger companies may have less complex units. Factors that might indicate less complex operations include: fewer business lines; less complex business processes and financial reporting systems; more centralized accounting functions; extensive involvement by senior management in the day-to-day activities of the business; and fewer levels of management. (AS 5, ¶9.)

Materiality

As in the financial statement audit, the concept of materiality is key to the audit of internal controls. Thus, in planning the audit of internal controls, auditors should use the same materiality considerations they would use in planning the audit of the company's annual financial statements. (AS 5, ¶20.)

The Board does not believe that an auditing standard on internal controls is an appropriate place to either redefine or refine the meaning of materiality, which is a long-established concept in the federal securities laws.

Under AS 5, auditors should use the same consideration of account-level materiality in determining the nature, timing, and extent of their procedures in the audit of internal controls as used in the financial statement audit. Similarly, since inherent risk is also the same for both audits, significant accounts identified in the internal control audit should be the same as the significant accounts identified in the financial statement audit.

Risk Assessment

Risk assessment underlies the entire audit process mandated by AS 5, including the determination of significant accounts and disclosures and relevant assertions, the selection of controls to test, and the determination of the evidence necessary for a given control. (AS 5, ¶10.) The standard thus requires risk assessment at each of the decision points in a top-down approach.

AS 5 defines "relevant assertions" as those financial statement assertions that have a reasonable possibility of containing a misstatement that would cause the financial statements to be materially misstated. The determination of whether an assertion is a relevant assertion is based on inherent risks, without regard to the effect of controls. (AS 5, ¶A9.)

In the Board's view, focusing auditor attention on the areas of greatest risk is likely to produce a more effective audit and substantially decrease the opportunity for a material weakness to go undetected. The proper use of risk assessment also enhances audit efficiency because the auditor does not spend time testing controls that, even if deficient, would not present a reasonable possibility of material misstatements in the financial statements.

Moreover, a direct relationship exists between the degree of risk that a material weakness could exist in a particular area of the company's internal controls and the amount of audit attention that should be devoted to that area. In addition, the risk that a company's internal controls will fail to prevent or detect misstatement caused by fraud usually is higher than the risk of failure to prevent or detect error. Auditors should focus more of their attention on the areas of highest risk. On the other hand, it is not necessary to test controls that, even if deficient, would not present a reasonable possibility of material misstatements. (AS 5, ¶11.)

The complexity of the organization, business unit, or process plays a key role in the auditor's risk assessment and the determination of the necessary procedures. (AS 5, ¶12.)

Top-Down Approach

Under the top-down approach embodied in AS 5, the auditor must test those controls that address the assessed risk of misstatement to each relevant assertion. These are the most important controls to test.

As a practical matter, the auditor will generally need to understand the company's processes to appropriately identify the correct controls to test. The Board believes, however, that specific requirements directing the auditor how to obtain that understanding are unnecessary and could contribute to a checklist approach to compliance, particularly for auditors who have a longstanding familiarity with the company. Thus, the Board has removed the requirements to identify major classes of transactions and significant processes from the final standard.

When using a top-down approach, the auditor identifies the controls to test by starting at the top, which is the financial statement and the entity-level controls. A top-down approach first begins at the financial statement level and with the auditor's understanding of the overall risks to internal controls. Note that the top-down approach describes the auditor's sequential thought process in identifying risks and the controls to test, not necessarily the order in which the auditor will perform the auditing procedures.

The auditor next focuses on entity-level controls and works down to significant accounts and disclosures and their relevant assertions. This approach directs the auditor's attention to accounts, disclosures, and assertions that present a reasonable possibility of material misstatement to the financial statements. Auditors must then verify their understanding of the risks in the company's processes and select for testing those controls that sufficiently address the assessed risk of misstatement to each relevant assertion. (AS 5, ¶21.)

Entity-level controls are crucial to the auditor's ability to appropriately tailor the audit through a top-down approach, specifically by identifying and testing the most important controls. Entity-level controls, formerly called company-level controls, can also reduce the testing of other controls related to a relevant assertion. This is either because the entity-level control sufficiently addresses the risk related to the relevant assertion, or because they provide some assurance so that the testing of other controls related to that assertion can be reduced.

In order to clarify these concepts, AS 5 includes a discussion of three broad categories of entity-level controls, which vary in nature and precision, along with an explanation of how each category might have a different effect on the performance of tests of other controls. The three categories are: control environment controls; controls monitoring the effectiveness of other controls; and controls adequately preventing or detecting misstatements to relevant assertions.

The standard explains that some controls, such as certain control environment controls, have an important, but indirect effect on the likelihood that a misstatement will be detected or prevented on a timely basis. These controls might affect the other controls the auditor selects for testing and the nature, timing, and extent of procedures the auditor performs on other controls.

The standard also explains that other entity-level controls may not operate at the level of precision necessary to eliminate the need for testing of other controls, but can reduce the required level of testing of other controls, sometimes substantially. This is because the auditor obtains some of the supporting evidence related to a control from an entity-level control and the remaining necessary evidence from the testing of the control at the process level.

Controls that monitor the operation of other controls are the best example of these types of controls. These monitoring controls help provide assurance that the controls that address a particular risk are effective and, therefore, they can provide some evidence about the effectiveness of those lower-level controls, reducing the testing of those controls that otherwise would be necessary.

The standard notes that some entity-level controls might operate at a level of precision that, without the need for other controls, sufficiently addresses the risk of misstatement to a relevant assertion. If a control sufficiently addresses the risk in this manner, the auditor does not need to test other controls related to that risk.

The Board has noted that the identification of risks and controls within IT is not a separate evaluation. Instead, it is an integral part of the top-down approach used to identify significant accounts and disclosures and their relevant assertions, and the controls to test, as well as to assess risk and allocate audit effort. (AS 5, ¶36.)

Period-end Financial Reporting Process

Because of its importance to financial reporting and to the auditor's opinions on internal controls and the financial statements, the auditor must evaluate the period-end financial reporting process. Under AS 5, the period-end financial reporting process includes:

- Procedures used to enter transaction totals and record journal entries into the general ledger;
- Procedures related to the selection and application of accounting policies;
- Procedures used to prepare financial statements and record adjustments to them.

It should be noted that, because the annual period-end financial reporting process normally occurs after the as-of date of management's assessment, those controls usually cannot be tested until after the as-of date.

As part of evaluating the period-end financial reporting process, the auditor should assess:

- Inputs, procedures performed, and outputs of the processes the company uses to produce its financial statements;
- The extent of information technology involvement in the period-end financial reporting process;
- Who participates from management and the nature of management and audit committee oversight;
- The locations involved in the period-end financial reporting process; and
- The types of adjusting and consolidating entries.

AS 5 demands that the auditor obtain sufficient evidence of the effectiveness of those quarterly controls that are important to determining whether the company's controls sufficiently assess the risk of misstatement to each relevant assertion as of the date of management's assessment. However, the auditor is not required to obtain sufficient evidence for each quarter individually. (AS 5, ¶27.)

Identifying Significant Accounts

Another aspect of planning the audit is identifying significant accounts and disclosures and their relevant assertions. The financial statement assertions include:

- Existence or occurrence
- Completeness
- Valuation or allocation
- Rights and obligations
- Presentation and disclosure

The Board noted that auditors may base their work on assertions that differ from those in AS 5 if they selected and tested controls over the pertinent risks in each significant account and

disclosure that have a reasonable possibility of containing misstatements that would cause the financial statements to be materially misstated.

In identifying significant accounts and disclosures and their relevant assertions, auditors should evaluate risk factors related to the financial statement line items and disclosure, including the size and composition of the account, the volume of activity, accounting complexities, any related party transactions, and the susceptibility to misstatement due to errors or fraud. (AS 5, ¶29.)

The auditor should also determine the likely sources of potential misstatements that would cause the financial statements to be materially misstated. Auditors might determine the likely sources of potential misstatements by asking themselves "what could go wrong?" with a given significant account or disclosure. (AS 5, ¶30.)

When a company has multiple locations or business units, auditors should identify significant accounts and disclosures and their relevant assertions based on the consolidated financial statements. After making those determinations, auditors should apply the Board's direction for multiple locations scoping decisions. (AS 5, ¶33.) Essentially this would mean assessing the risk of material misstatement in a financial statement associated with the location or business unit and correlating the amount of audit attention devoted to the location or unit with the degree of risk. (AS 5, ¶B10.)

Understanding the Sources of Misstatements

AS 5 commands auditors to try to understand the likely sources of potential misstatements in company financials by understanding the flow of transactions and identifying the points in the internal control processes at which a material misstatement could arise. Auditors should also identify controls that management has implemented to address potential misstatements, as well as controls designed to prevent the unauthorized use or disposition of company assets that could result in a misstatement. (AS 5, ¶34.)

Because of the degree of judgment required, auditors must either perform the procedures to understand potential sources of misstatements themselves or supervise the work of others who provide direct assistance to the auditors. (AS 5, ¶35.)

Testing the Controls

AS 5 mandates that auditors test controls that are important to their conclusion about whether the company's controls sufficiently address the assessed risk of misstatement. The Board recognizes that there might be more than one control that addresses the risk of misstatement; while conversely one control might address the risk of misstatement to more than one relevant assertion.

It is neither necessary to test all controls related to a relevant assertion nor necessary to test redundant controls. Further, the decision on selecting a control for testing depends on which controls sufficiently address the assessed risk of misstatement rather than on how the control is labeled, such as entity-level control or transaction-level control. (AS 5, ¶s 39, 40 and 41.)

Auditors must test both the operating effectiveness and design effectiveness of the company's internal controls. Procedures testing design effectiveness would include a mix of inquiry of appropriate personnel, observation of the company's operations, and the inspection of documentation. The Board believes that walkthroughs that include these procedures ordinarily are sufficient to evaluate design effectiveness. Procedures testing operating effectiveness would include a mix of inquiry of appropriate personnel, observation of the company's operations, inspection of relevant documentation, and re-performance of the control. (AS 5, ¶s 42 through 45.)

Role of Risk

For each control selected for testing, the evidence necessary to persuade the auditor that the control is effective depends on the risk that the control will not be effective and that a material weakness would result. As the risk associated with the control being tested increases, the evidence that the auditor should obtain also increases. But note that, although the auditor must obtain evidence about the effectiveness of controls for each relevant assertion, the auditor is not responsible for obtaining sufficient evidence to support an opinion about the effectiveness of each individual control.

Rather, the auditor's objective is to express an opinion on the company's internal controls. This allows the auditor to vary the evidence obtained regarding the effectiveness of individual controls selected for testing based on the risk associated with the individual control. (AS 5, ¶46.)

AS 5 lists a number of factors affecting the risk associated with a control, including the nature of misstatements the control is intended to prevent, the inherent risk associated with related accounts, the complexity of controls, the competence of the people monitoring the control, and the degree to which the control relies on the effectiveness of other controls. Another risk factor is whether the control is automated or relies on an individual's performance since the Board believes that an automated control will generally be lower risk so long as the IT general controls are effective. (AS 5, ¶47.)

The Board has noted that a less complex company or business unit with simple business processes and centralized accounting operations might have relatively simple information systems that make greater use of off-the-shelf packaged software without modification. In the areas in which off-the-shelf software is used, the auditor's testing of information technology controls might focus on the application controls built into the pre-packaged software that management relies on to achieve its control objectives and the IT general controls that are important to the effective operation of those application controls. (AS 5, ¶47.)

Control Testing Principles

AS 5 also sets forth a number of general principles with regard to the testing of controls:

- A conclusion that a control is not operating effectively can be supported by less evidence than a conclusion that it is effective.
- Re-performance of a control is greater evidence of effectiveness than observation, inspection of documentation, or inquiry.
- Inquiry alone cannot provide enough evidence to support a conclusion on a control's effectiveness.
- Documentary evidence of the operation of some controls, such as management's philosophy, might not exist.
- Testing controls over a greater period time provides more evidence of effectiveness.
- Testing controls closer to the date of management's assessment provides more evidence than testing earlier in the year
- The more extensively a control is tested, the greater the evidence obtained from that test.

Multi-Location Testing

Companies with multiple locations or business units present the auditor with additional decision points when planning and performing the audit. The PCAOB has refocused the standard's multi-location testing requirements on risk rather than coverage or coverage ratios. Thus, the Board has dropped the provision requiring the testing of controls over a large portion of the company. Instead, auditors will now employ a risk-based approach in determining the proper strategy for auditing multiple locations. The flexibility provided by this approach allows auditors to exercise the necessary judgment in the particular circumstances and should result in more efficient multi-location audits.

In determining the locations or business units at which to perform tests of controls, the auditor will assess the risk of misstatement to the financial statements associated with the location or business unit and correlate the amount of audit attention devoted to the location or business unit with the degree of risk. The auditor may eliminate from further consideration those locations or business units that, individually or when aggregated with others, do not present a reasonable possibility of misstatement to the consolidated financial statements. (AS 5, ¶B10.)

In assessing and responding to risk, the auditor should test controls over specific risks that present a reasonable possibility of material misstatement to the consolidated financial statements. In lower-risk locations or business units, the auditor first might evaluate whether testing entity-

level controls, including controls in place to provide assurance that appropriate controls exist throughout the organization, provides the auditor with sufficient evidence. (AS 5, ¶B11.)

Further, in determining the locations or business units at which to perform tests of controls, the outside auditors may take into account work performed by others on behalf of management. For example, if the internal auditors' plan relevant audit work at various locations, the independent auditors may coordinate work with the internal auditors and reduce the number of locations or business units at which they would otherwise need to perform auditing procedures. (AS 5, ¶B12.)

Using Earlier Audits

AS 5 allows auditors to incorporate the knowledge they obtained during past audits of the company's internal controls over financial reporting into the nature, timing, and extent of testing necessary for a current audit. This principle may allow auditors to reduce testing in later years. Auditors are cautioned, however, to be aware of any changes in the control or the process in which it operates since the previous audit. (AS 5, ¶s 57 and 58.)

Auditors are also permitted to use a benchmarking strategy for automated application controls in subsequent years' audits. (AS 5, ¶60.) Benchmarking involves establishing a baseline and verifying that the automated control has not changed since the baseline's establishment. This would allow the auditor to conclude that the automated control is still effective without repeating the prior year's tests. (AS 5, ¶B29.)

Auditor's Opinion

The auditor should form an opinion on the effectiveness of internal control over financial reporting by evaluating evidence obtained from all sources, including the auditor's testing of controls, misstatements detected during the financial statement audit, and any identified control deficiencies. As part of this evaluation, the auditor should review reports issued during the year by internal audit on the internal controls. Further, after forming an opinion on the effectiveness of the company's internal controls, the auditor should evaluate the presentation of the elements that management is required, under SEC rules, to present in its annual report on internal controls. (AS 5, ¶s 71 and 72.)

If the auditors determine that any required elements of management's annual report on internal controls are incomplete or improperly presented, the auditors must modify their report to include an explanation describing the reasons for this determination. (AS 5, ¶s 73 and C2.)

Importantly, the auditor may form an opinion on the effectiveness of internal controls only when there have been no restrictions on the scope of the auditor's work. A scope limitation requires the auditor to disclaim an opinion or withdraw from the engagement. In an audit of internal controls, the auditor should also obtain the following written representations from management:

- Acknowledging management's responsibility for maintaining effective internal controls;
- Stating that management has performed an evaluation and made an assessment of the effectiveness of the internal controls;
- Stating that management did not use the auditor's procedures performed during its internal control audit as part of the basis for management's assessment of the effectiveness of the internal controls;
- Stating management's conclusion about the effectiveness of the internal controls based on the control criteria as of a specified date;
- Stating that management has disclosed to the auditor all deficiencies in the design or operation of internal controls identified as part of management's evaluation, including separately disclosing to the auditor all significant deficiencies or material weaknesses;
- Describing any fraud resulting in a material misstatement to the financial statements and any other fraud involving senior management or management or other employees who have a significant role in the company's internal controls over financial reporting;
- Stating whether control deficiencies identified and communicated to the audit committee during previous engagements have been resolved, and specifically identifying any that have not; and
- Stating whether there were, subsequent to the date being reported on, any changes in internal controls or other factors that might significantly affect internal controls, including any corrective actions taken by management with regard to significant deficiencies and material weaknesses. (AS 5, ¶75.)

Note that the failure to obtain these written representations from management, including management's refusal to furnish them, constitutes a limitation on the scope of the audit such that the auditor should either withdraw from the engagement or disclaim an opinion. Further, auditors should evaluate the effects of management's refusal on their ability to rely on other representations, including those obtained in the audit of the company's financial statements. (AS 5, ¶76.)

Auditor's Report

The auditor may choose to issue a combined report, that is, one report containing both an opinion on the financial statements and an opinion on the internal controls, or separate reports on the company's financial statements and on the internal controls. (AS 5, ¶86.) Further, auditors should date the report no earlier than the date on which they have obtained sufficient competent

evidence to support their opinion. Because the auditor cannot audit internal control over financial reporting without also auditing the financial statements, the reports should be dated the same. (AS 5, ¶89.)

The auditor's report on the audit of internal control over financial reporting must include the following elements:

- A title that includes the word *independent*;
- A statement that management is responsible for maintaining effective internal controls and for assessing the their effectiveness;
- An identification of management's report on internal controls;
- A statement that the auditor's responsibility is to express an opinion on the company's internal controls based on the audit;
- A definition of internal control over financial reporting as stated in AS 5;
- A statement that the audit was conducted in accordance with PCAOB standards;
- A statement that the PCAOB standards require that the auditor plan and perform the audit to obtain reasonable assurance about whether effective internal controls were maintained in all material respects;
- A statement that an audit includes obtaining an understanding of internal controls, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as the auditor considered necessary in the circumstances;
- A statement that the auditor believes the audit provides a reasonable basis for his or her opinion;
- A paragraph stating that, because of inherent limitations, internal controls may not prevent or detect misstatements;
- The auditor's opinion on whether the company maintained, in all material respects, effective internal controls as of the specified date,
- The manual or printed signature of the auditor's firm; and
- The city and state (or city and country, in the case of non-U.S. auditors) from which the auditor's report has been issued.

Material Weaknesses

As noted, when material weaknesses exist, the auditor must express an adverse opinion on the company's internal control over financial reporting, unless there is a restriction on the scope of the engagement. When expressing this adverse opinion, the report must include the PCAOB's definition of material weakness and a statement that a material weakness has been identified and an identification of the material weakness in management's assessment. (AS 5, ¶91.)

If the material weakness has not been included in management's assessment, the report should be modified to state that a material weakness has been identified but not included in management's assessment. Additionally, the auditor's report should include a description of the material weakness, which should provide the users of the audit report with specific information about the nature of the material weakness and its actual and potential effect on the presentation of the company's financial statements issued during the existence of the weakness.

In this case, the auditor also should communicate in writing to the audit committee that the material weakness was not disclosed or identified as a material weakness in management's assessment. If the material weakness has been included in management's assessment but the auditor concludes that the disclosure of the material weakness is not fairly presented in all material respects, the auditor's report should describe this conclusion as well as the information necessary to fairly describe the material weakness.

Finally, auditors should determine the effect that their adverse opinion on internal control has on their opinion on the financial statements and disclose whether their opinion on the financial statements was affected by their adverse opinion on the internal controls. (AS 5, ¶92.)

Modifying the Report

AS 5 requires auditors to modify their internal control report in the following five circumstances:

1. *Management's Report on Internal Controls is Incomplete or Improper*. In this circumstance, the auditor should modify its report to include an explanation describing the reasons for this determination.

2. *Limitations on the Scope of the Audit*: If there are restrictions on the scope of the internal control engagement, the auditor should withdraw from the engagement or disclaim an opinion on the effectiveness of the internal controls. Management and the audit committee should be told in writing that the internal control audit cannot be completed because of the scope limitation.

3. *Opinions Based on Another Auditor's Report*. When another auditor has audited the financial statements and internal controls of one of the company's subsidiaries or divisions, and the auditor makes reference to it as a basis for an opinion on the internal controls, the auditor should refer to the other auditor's opinion

4. *Management's Report on Internal Controls Contains Additional Information*. In this circumstance, if management's report could reasonably be viewed by users of the report as including such additional information, the auditor should disclaim an opinion on the information.

5. *Management's sec. 302 certification is misstated*. If the auditor believes that modifications to disclosures about changes in internal controls are necessary for the accuracy of the Sarbanes-Oxley 302 certifications, and management and the audit committee fail to appropriately respond, the auditor's report should include an explanation describing the reasons the auditor believes management's disclosures should be modified. (AS 5, ¶s C1 through C15.)

Post-Audit Events

The Board recognizes that changes in the internal controls can occur after the audit but before the date of the auditor's report. The auditor should inquire of management whether there were any such changes and obtain written representations from management relating to such matters.

To obtain additional information about whether changes have occurred that might affect the effectiveness of the internal controls and therefore the auditor's report, the auditor should inquire about and examine, for this subsequent period, the following:

- Relevant internal audit reports issued during the subsequent period,
- Independent auditor reports of deficiencies in internal control, and
- Regulatory agency reports on the company's internal controls.

If the auditor obtains knowledge about subsequent events that materially and adversely affect the effectiveness of the company's internal controls, AS 5 mandates that the auditor issue an adverse opinion on internal control over financial reporting. If the auditor is unable to determine the effect of the subsequent event on the effectiveness of the company's internal controls, the auditor should disclaim an opinion. (AS 5, ¶96.)

Congressional Reaction

Reacting to the SEC guidance, Senate Banking Committee Chair Christopher Dodd said that the Commission is attempting to further the goals of Sarbanes-Oxley while improving its regulatory implementation and reducing unnecessary costs. While commending the SEC's efforts the oversight chair pledged to fully and thoroughly review the SEC regulations.

His remarks come against the backdrop of the recent Dodd-Shelby amendment to the American Competes Act (S. 761), which gave the SEC and PCAOB more time, but not unlimited time, to reform the internal control reporting mandates under Section 404 of the Sarbanes-Oxley Act. Specifically, the amendment, which passed 97-0, expressed the sense of the Senate that the SEC and PCAOB should implement the Section 404 mandates in a manner that limits the burdens placed on small and mid-size public companies. The amendment was introduced by Sen. Dodd (D-Conn.) and co-sponsored by Sen. Richard Shelby (R-AL), the committee's Ranking Member. The Senate passed S 761 by a vote of 88-8.

The Senate also supported a Dodd-Shelby motion to table an amendment offered by Sen. Jim DeMint (R-SC). The DeMint amendment would have made Section 404 compliance optional for smaller companies with market capitalization of less than $700 million, with revenue of less than $125 million, or with fewer than 1,500 shareholders, thereby exempting over 70% of companies from key parts of Sarbanes-Oxley. This amendment was tabled on a bipartisan vote of 62-35.

By these two votes, the Senate made a strong statement in two respects, according to Sen. Dodd. First, that the Senate will continue to protect investors in public companies; and second, that it supports efforts currently underway to ensure that small and mid-size businesses are not unduly burdened by rules intended to protect investors. The Senate rejected an approach that would weaken investor protection and make it more likely for investors to be harmed by the malfeasance that caused the collapse of Enron and WorldCom.

For his part, Sen. Shelby observed that the SEC guidance and new PCAOB standard are mutually reinforceable and should significantly improve the implementation of Section 404, making it more efficient and effective for small and medium-sized businesses. That is what the Senate wants. The Ranking Member is buoyed by the fact that the agencies recognize that the unnecessary costs imposed by Section 404 are a real problem for both large and small companies

Importantly, the Dodd-Shelby amendment endorsed Section 404 for greatly enhancing the quality of corporate governance and financial reporting for public companies and increasing investor confidence. It praised the SEC and PCAOB for determining that the auditing standard implementing Section 404, AS 2, has imposed unnecessary and unintended cost burdens on small and mid-sized public companies.

Sen. Dodd emphasized that the SEC Chair has wide latitude within which to operate here, since the statute gives broad discretion. The Dodd-Shelby amendment agreed with recent statements by SEC Chair Christopher Cox that Sarbanes-Oxley did not need to be amended, but that the regulators need to change the way the law is implemented. It is the implementation of the law that has caused the excessive burden, reasoned the chair, not the law itself.

Sen. Dodd agrees that Sarbanes-Oxley should not be opened up to an amendment at this time. Indeed, he believes that it would be irresponsible for Congress at this juncture to jump in and

greatly reduce the number of companies that would have to comply with Section 404. The SEC must be allowed to do its job, he emphasized. If the Commission does not do the job, he continued, and the burdens of Section 404 still exist, the senator would welcome an opportunity to address that. In his view, the amendment sends a message to the SEC and the PCAOB that the Senate is watching what they do very carefully.

For his part, Sen. Shelby was also willing to give the SEC and PCAOB time to make the significant changes needed to reduce the unacceptable costs and burdens 404 compliance. The problems are complex, he added, and the regulators should be given a chance to fix them. While Sen. Shelby is willing to give the SEC and PCAOB some additional time to fix the problem, he is not willing to give them unlimited time. He said that the Banking Committee will monitor closely their progress and hold them accountable should there be any unnecessary delays.

Small Business Committee

Viewing the SEC's action, Senators John Kerry (D-Mass.) and Olympia Snowe expressed strong concern that the Commission failed to provide an extension for small public companies to comply with the Sarbanes-Oxley internal control regulations. Kerry and Snowe, the Chair and Ranking Member of the Small Business Committee, seek up to one additional year for small businesses to comply with the law. According to Sen. Kerry, it will take some time to fully assess how the SEC's final rules will impact small public companies, as "the devil is in the details." However, he is disappointed that the SEC chose not to honor the request for an extension of the compliance deadline for small businesses.

Without the extension, non-accelerated filers must file their management's assessments with their annual reports closing on or after December 15, 2007.

While pleased with the SEC's management guidance, Sen. Snowe remains concerned that the SEC has provided no assurances that the new internal controls rules will actually reduce costs for small companies because they have not yet completed the required Regulatory Flexibility Act review of the rule. She is also disappointed that the SEC has not granted small companies a one year delay in their filing requirements nor issued a small business compliance guide to assist small firms in coming up to speed with these new regulations.