SARBANES-OXLEY SECTION 404:

A Guide for Management by Internal Controls Practitioners

PROFESSIONAL GUIDANCE

Setting the Standard

SARBANES-OXLEY SECTION 404:

A Guide for Management by Internal Controls Practitioners

The Institute of Internal Auditors
2nd Edition, January 2008

Table of Contents

About the Second Edition

This is an updated version of The Institute of Internal Auditor's (IIA's) *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners*, one of its most frequently downloaded products. Changes include:

- Updated references to Auditing Standard No. 5 (AS 5) and the U.S. Securities and Exchange Commission's (SEC's) guidance for management on Section 404 of the U.S. Sarbanes-Oxley Act of 2002. The first edition was based on the top-down and risk-based approach adopted in both documents, and the second edition updates the discussion and extends the guidance provided by the regulators.
- An expanded and updated discussion of information technology (IT) general controls scoping based on The Institute's Guide to the Assessment IT General Controls Scope Based on Risk (GAIT) products.
- An extended discussion of the role of entity-level controls.
- The benefit of additional years of experience with management's assessment of internal control over financial reporting (ICFR).

The approach discussed in this guide has proven successful over the last few years, streamlining management's processes, and effecting major reductions in total assessment cost.

How to Use This Guide

Organizations can use this guide to ensure their program for assessing the system of internal control over financial reporting is not only effective but also cost-effective. They will use this guide to:

- Supplement and extend the guidance for management that has been provided by the SEC.
- Assess the efficiency of their Section 404 program, such as how to minimize total assessment costs, including related external auditor fees.
- Revisit their assessment process and compare it to best practices identified by experienced internal control practitioners.
- Reconsider their processes for assessing deficiencies and providing an overall opinion. Management should provide an opinion that is based on principles instead of rules (i.e., an opinion that provides the investor with a fair assessment of the system of internal control). It should reflect the true condition of the internal control system, not one based on technicalities that could mislead the investor who needs to have confidence in the financial reports.

Based on their role in their organization and responsibilities for Section 404, readers may use the guide in its entirety or read specific sections based on interest.

The first and last sections — the "Summary for the CEO and CFO" and "Closing Thoughts on Efficiency" — merit all readers' consideration.

Introduction

Various organizations have provided guidance on the subject of Section 404 and management's annual assessment of its system of ICFR.

- The U.S. Public Company Accounting Oversight Board (PCAOB) provided an updated standard for external auditors in May 2007: AS 5, *An Audit of Internal Control Over Financial Reporting That Is Integrated With an Audit of Financial Statements*.
- Management actions are governed by the SEC and not the PCAOB. While the SEC endorsed AS 5, it also provided its own *Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting Under Section 13(a) or 15(d) of the Securities Exchange Act of 1934* in June 2007. This high-level guidance is not mandatory for management, but following it provides a safe harbor.
- Each of the major certified public accounting (CPA) firms and other providers of audit services have published extensive and valuable guidance, generally consistent with PCAOB and SEC guidance.

As noted above, following the SEC's guidance provides management with a safe harbor. However, the guidance is at a high level and management may find additional, more detailed assistance is required. This document provides that additional level of assistance.

The guide includes frequent references not only to SEC guidance but also to PCAOB guidance as the greater level of detail in the latter is often helpful. In addition, as discussed later, it may be easier to obtain a higher level of external auditor reliance on management's testing if management's and the auditor's approaches are aligned.

Internal auditors specialize in the assessment of internal controls and have for decades. They do so as a service to their organization's audit committee and senior management team, and, therefore, have extensive insight into the operation of those controls and the constraints on management in providing those controls. They are experts in the theory and practice of internal controls and related auditing.

This guide — which is produced by The IIA, the recognized authority and standard-maker for internal auditing in the United States and around the world — is written for management by experienced internal auditors who have worked on internal controls hand-in-hand with the board and management.

The guide incorporates and reflects up-to-date guidance from the SEC, the PCAOB, The IIA, and the real-world experience and insight of practicing internal auditors.

Because cost is an issue for all management teams, this guide focuses especially on how total assessment costs, including related external audit fees, can be minimized without impairing the effectiveness of the program.

The guide also discusses the interplay between the requirements of Section 404 and those of Section 302. The latter requires annual and quarterly certifications by the chief executive officer (CEO) and chief financial officer (CFO)[i] that include assessments of internal controls.

We encourage readers to review their Section 404 program with the head of their internal audit function, especially how the program ensures efficiency and minimizes disruption to the business. The internal auditor is uniquely positioned not only to review and test the key controls but also to provide internal consulting on the adequacy of their design and on the entire management assessment and testing process. To this end, this guide contains a checklist that may be of value in assessing the efficiency of the program.

Summary for the CEO and CFO

When the U.S. Congress passed the Sarbanes-Oxley Act, the intent was to drive improvements in companies' internal controls. The benefits were seen as greater assurance to shareholders and other stakeholders in published financial reports, while compliance costs were of lesser significance and were dramatically underestimated.

However, cost is of tremendous importance to corporate executives. While they have an obligation to provide an effective system of internal control that provides assurance regarding the integrity of financial reporting and the safeguarding of assets, there should be a balance between the cost of those controls and the risks they are managing.

Managers who are responsible for their company's Section 404 program can obtain the following benefits from this guide, which is focused on achieving success at the lowest possible total cost, including external auditor fees:

- A clear understanding of the requirements of the Sarbanes-Oxley Act and the fundamentals of internal controls.
- A discussion of how the annual requirements of Section 404 relate to the quarterly requirements of Section 302 (i.e., the quarterly certification by the CEO and CFO).
- An explanation and practical suggestions for each phase of the program, including areas of difficulty: the identification of key controls, assessing deficiencies, and the final assessment.
- Advice on how to reach a fair assessment that does not mislead investors regarding the condition of internal controls and the reliability of financial statements. We believe management's formal assessment should reflect their belief as to whether the system of internal control provides reasonable assurance of the reliability of *future*[1] financial statements.[ii] That reliability is based on the likelihood of an error that would be material to a reasonable investor. An assessment that the controls are not effective simply because there has been a restatement of previously issued financial statements may mislead the investor regarding the current state of internal controls and the reliability of future financial statements.

1 The guidance published by the SEC and PCAOB does not address this issue directly. However, there are indications in comments by officials with these organizations that the value of the Section 404 assessment is that it provides a level of comfort with respect to the reliability of future financial statements assuming there is no significant change in the quality of the system of internal control. The quality of the system of internal control at the end of the reporting year is an indication of whether it is sufficiently robust to either prevent or detect material misstatements in financial statements that will be prepared under the processes and related controls that management has assessed. In addition, an assessment of the likelihood of any event is difficult, if not impossible, without defining the period during which the event may occur. In this guide, we have taken the reasonable position that management's assessment should reflect the likelihood of a material misstatement in one or more of the next 12 months' financial statement filings. Neither the SEC nor the PCAOB have publicly commented on this matter, and our position relative to 12 months — which would include the next annual financials on Form 10-K as well as interim reports on Form 10-Q — is a suggestion based on what we believe is reasonable.

- A checklist to help management assess the efficiency of their program.
- Some companies have adopted a methodology for Section 404 that is rules-based.[iii] This can lead to an assessment that is neither effective nor efficient. Instead, management should use judgment to develop and operate a continuing Section 404 program that is principles-based. Executives should understand that:
  - Management has a great deal of flexibility in designing and implementing their Section 404 program — much more than is available to the external auditor.[iv]
  - Both management and the external auditor have been encouraged by the SEC and the PCAOB to use their judgment and develop an approach that is top-down and risk-based. The Section 404 program should include coverage of all areas where the inherent risk (i.e., the risk before the quality of internal controls is considered) of an error that could lead to a material misstatement[v] is at least reasonably possible.[vi] There is no need for the program to assess and test every control related to financial reporting, even those that might be considered significant deficiencies if they failed (see the definition of "significant deficiency" provided later in this guide).

KEY POINTS

MANAGEMENT'S ROLE

- *Management has a great deal of flexibility in designing and implementing their Section 404 program — much more than is available to the external auditor.*

On May 16, 2005, the SEC staff issued a *Statement on Management's Report on Internal Control Over Financial Reporting* that said (emphasis added):

> "An overall purpose of internal control over financial reporting is to foster the preparation of reliable financial statements. Reliable financial statements must be materially accurate. Therefore, a central purpose of the assessment of internal control over financial reporting is to identify material weaknesses that have, as indicated by their very definition, more than a remote likelihood of leading to a material misstatement in the financial statements. While identifying control deficiencies and significant deficiencies represents an important component of management's assessment, *the overall focus of internal control reporting should be on those items that could result in material errors in the financial statements*.
>
> "In adopting its rules implementing Section 404, the Commission expressly declined to prescribe the scope of assessment or the amount of testing and documentation required by management. *The scope and process of the assessment*

KEY POINTS

SEC STAFF STATEMENT

- *"The overall focus of internal control reporting should be on those items that could result in material errors in the financial statements."*
- *"Management should not allow the goal and purpose of the internal control over financial reporting provisions — the production of reliable financial statements — to be overshadowed by the process."*

should be reasonable, and the assessment (including testing) should be supported by a reasonable level of evidential matter. "Each company should also use informed judgment in documenting and testing its controls to fit its own operations, risks, and procedures. Management should use its own experience and informed judgment in designing an assessment process that fits the needs of that company. Management should not allow the goal and purpose of the internal control over financial reporting provisions — the production of reliable financial statements — to be overshadowed by the process."

Similarly, AS 5[vii] directs the external auditor to focus on the risk of material errors:

"The auditor's objective in an audit of internal control over financial reporting is to express an opinion on the effectiveness of the company's internal control over financial reporting. Because a company's internal control cannot be considered effective if one or more material weaknesses exist, to form a basis for expressing an opinion, the auditor must plan and perform the audit to obtain competent evidence that is sufficient to obtain reasonable assurance about whether material weaknesses exist as of the date specified in management's assessment."

In April 2007, the PCAOB released a report on their inspections of external auditors' work on internal controls over financial reporting.[viii] Their findings included:

KEY POINTS

PCAOB FINDINGS

- *Some auditors did not fully integrate their audits.*
- *Some auditors failed to apply a top-down approach to testing controls.*

"In 2006, Board inspectors reviewed portions of approximately 275 audits of internal control over financial reporting ('internal control') conducted in the second year of implementation of AS No. 2. These inspections revealed that progress was made in improving the efficiency of internal control audits. Many of these improvements resulted from the easing of time constraints that auditors and issuers faced in the first year, issuers' and auditors' additional experience, and changes that auditors made in their methodologies and staff training."

"In the 2006 inspections, the inspectors found evidence that most firms had made progress in integrating their audits (for example, by using the same engagement team to perform both the financial statement audit and the audit of internal control over financial reporting). The inspectors also observed more instances in which auditors approached the audit of internal control from the top down and thus did a better job of focusing their testing and evaluation on the relevant company-level controls. As a result, they spent less time testing a larger number of controls that existed at the process, transaction, and application levels. Several of the firms achieved greater efficiencies by varying the extent of their testing commensurate with the level of risk and, generally, auditors used the work of others more in the second year of implementing AS No. 2 than in the first year."

"In each of the four areas on which the inspection teams focused, the reviews identified ways in which auditors could have been more efficient. While these observations varied in form and degree among the firms and engagement teams, the lessons learned can benefit auditors generally. The most common observations were:

- Some auditors did not fully integrate their audits.
- Some auditors failed to apply a top-down approach to testing controls.
- Some auditors assessed the level of risk only at the account level and not at the assertion level. As a result, those auditors likely expended more effort than necessary when testing controls for assertions that were lower risk. In a few cases, auditors tested the same controls that the issuer had tested, without assessing whether this was necessary to sufficiently address the risk that a relevant assertion might be misstated.
- Some auditors could have increased their use of the work of others."

Executives should also understand that:

- Management is **not** required to adopt the same methodology as the external auditor, although there may be advantages in using a similar approach. AS 5 is mandatory for external auditors, but not for management. However, management should give strong consideration to following the approach described in AS 5. One of the greatest sources of cost-savings is derived from maximizing the degree of reliance placed by the external auditor on management testing. When management and auditor use the same language and a consistent approach, reliance is easier to achieve.

  Management may elect to follow a different methodology than the external auditor. An emerging practice is for management and the auditor to review and reconcile the results of their two approaches. If the external auditor identifies key controls to test that are not included in management's scope, management may decide to add them. Even though management has determined they are not necessary, adding them to the scope might enable the external auditor to limit their independent testing and, as a result, reduce the company's total compliance cost.
- The regulators believed the greatest benefit from Section 404 was that it would provide greater assurance to investors and others that they could rely on management's published financials. The value of that assurance is not as it relates to the current set of financial statements (to which the Section 404 assessment is attached), as they are subject to a separate assertion by management and opinion by the external auditor on their adequacy. Neither is the value in assessing controls over prior period financials. The value is in providing comfort with respect to the reliability of financial statements that will be published in the *future*. The Section 404 assessment indicates to the investor whether the system of internal control is sufficiently robust such that the risk of material error in *future* financial statements is remote or less.[ix]

In practical terms, management's assessment of the system of ICFR should reflect whether they believe the risk of material misstatements in financial statements filed with the SEC over the next 12 months[1] is less than reasonably likely. An alternative view is whether management believes its system of ICFR contains any material weaknesses, representing a reasonable possibility that financial statements filed with the SEC over the next 12 months will contain material errors.

One of the greatest areas of potential cost-savings is through reduction of external costs (i.e., costs other than internal employees' time). Many companies continue to make significant use of third-party providers of consulting and audit services to perform testing and sometimes manage their Section 404 program; these companies are generally working to reduce costs by hiring project managers and testing personnel. In addition, external auditor fees related to their Section 404 work are typically significant.

In addition to the efficiencies they are gaining from experience, management can effect reductions in the cost of testing (both by management and by the external auditor) by:

- Limiting the number of key controls (i.e., the controls that have to be tested) by adopting a top-down, risk-based approach that focuses on controls that will prevent or detect material errors. Companies and external auditors have historically tested controls that are not key under this definition: that they are required to prevent or detect material errors. Controls that are not likely to result in material error should not be considered "key" and do not need to be within management's scope for Section 404.
- Using the top-down approach to identify direct entity-level controls (e.g., month-to-month payroll variance analyses performed during the period-end close process) that provide reasonable assurance that a material misstatement due to a failure in controls within the business process (e.g., within payroll) would be detected. In this situation, it may be possible to remove any business process controls from the scope of work.
- Maximizing reliance by the external auditor on management testing. This requires ensuring management testing is performed by skilled, experienced individuals who are independent of the activity being tested. The latter usually have several years' experience in a combination of external audit firms and internal auditing functions. Many companies use their internal audit function to perform the testing since this is the most likely approach to maximize external auditor reliance. Some use other internal staff to perform management testing and may rely on internal auditing to review and test their work to ensure it is to appropriate standards.[x]

KEY POINTS

COST MANAGEMENT

- *Use a top-down, risk-based approach to limit the number of key controls.*
- *Maximize reliance by the external auditor on management testing.*
- *Execute controls flawlessly.*

1 See the earlier footnote (1). Our recommendation is to use a period of 12 months. However, the SEC and PCAOB have not publicly commented on whether this is the appropriate period.

- Executing controls flawlessly. The tolerance level for defects in testing is very low. If the external auditors find even one error in their testing of a control, they may assess the control as not operating effectively. This will require remediation and retesting, potentially doubling the work.
- Documenting the processes and controls clearly and in good detail, and then ensuring the documentation is updated promptly as processes change.
- Completing a substantial portion of management's work, including testing all key controls (even if only limited in sample size) by mid-year. This enables the external auditors to start their work early, which helps with resource scheduling and reduces the risk of finding deficiencies late.

The above actions will also reduce management and employees' time maintaining documentation, assisting those performing the testing, etc.

In the past, most CEOs and CFOs have signed their annual and quarterly certifications — which are included in the financial statements filed with the SEC on Form 10-Q and required by Section 302 of Sarbanes-Oxley — without a rigorous examination of internal controls. Now that Section 404 is in force, management should be integrating its quarterly and annual assessment processes. Although management is not required to test all its key controls every quarter, they should perform some degree of testing each quarter to support the quarterly Section 302 certification.[xi] At a minimum, the Section 302 certification process should include a consideration of the status of the Section 404 project, the results of testing, the severity of any identified control deficiencies, and management's corrective action plans.

Companies, external audit firms, and the regulators are all learning how Section 404 should be applied and how both management and the external auditors can be both effective and efficient. The last section of this guide includes a number of questions management may use to assess their programs.

A. Section 404: Rules or Principles

Section 404 required the SEC to develop and publish rules for a management assessment of ICFR. These rules were completed in June 2003 and updated in June 2007. Changes included removing the requirement for the external auditor to assess management's process for assessing the system of ICFR, as well as revising the definitions of significant deficiency and material weakness. The PCAOB followed with AS 2, which was approved by the SEC in June 2004. AS 2 was replaced in May 2007 by AS 5.

The SEC rules and PCAOB standard require that:

1. Management perform a formal assessment of its controls over financial reporting (see definition below), including tests that confirm the design and operating effectiveness of the controls.
2. Management include in its annual report on Form 10-K[xii] an assessment of ICFR.
3. The external auditors provide two opinions as part of a single integrated audit of the company:
    a. An independent opinion on the effectiveness of the system of ICFR.
    b. The traditional opinion on the financial statements.

The SEC rules are worth reviewing carefully. They "require a company's annual report to include an internal control report of management that contains:

- A statement of management's responsibility for establishing and maintaining adequate internal control over financial reporting for the company.
- A statement identifying the framework used by management to conduct the required evaluation of the effectiveness of the company's internal control over financial reporting.
- Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the company's most recent fiscal year, including a statement as to whether or not the company's internal control over financial reporting is effective. The assessment must include disclosure of any "material weaknesses" in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the company's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting.
- A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting."

The "final rules also require a company to file, as part of the company's annual report, the attestation report of the registered public accounting firm that audited the company's financial statements."

Taking each point in turn:

1. Management is responsible for the system of internal control. This is an important clarification because some management teams believed[xiii] the system of internal control was the responsibility of the internal auditor, external auditor, or the CFO. By contrast, an effective system of internal control is the responsibility not just of the CFO but the CEO and the senior executive team as a whole.
2. The assessment has to be made using a recognized internal controls framework. Most U.S. companies have used the Committee of Sponsoring Organizations of the Treadway Commission (COSO) framework, although some have used the Control Objectives for Information and related Technology (COBIT) framework as a supplement to COSO for IT controls. (Both COSO and COBIT are discussed in section B below.)
3. The assessment is annual and as of year-end. There are restrictions on how management can make its assessment, depending on whether a material weakness is identified.
4. The external auditor must perform specified work in relation to management's assessment. The SEC mandated "an attestation report." The PCAOB has interpreted that in AS 5, with SEC consent, to be an independent assessment and formal opinion on the adequacy of the system of internal control over financial reporting.

While the PCAOB has provided detailed — and principles-based — guidance in AS 5 for external auditors, AS 5 is not binding on management. In fact, management has a great deal of flexibility in implementing its Section 404 program. The guidance from the SEC is also principles-based and at a fairly high level.

Management needs to understand AS 5 since it explains how the external auditor will review and evaluate management's assessment process. It is also important if management is going to minimize audit fees by maximizing reliance on management testing.

However, management also needs to ensure its process is faithful to the principles behind Section 404 — that it provides a fair assessment of its internal controls as of its year-end, reflecting whether the system provides reasonable assurance that material misstatements will be prevented or detected.

The following sections provide a road map for understanding the principles and requirements for Section 404 and implementing an efficient and effective Section 404 program. Section D explains the requirements of Section 302 (i.e., the quarterly certification by the CEO and CFO of the interim financials) and its relationship with Section 404.

B. Revisiting the Principles of Internal Control

There are a number of different definitions of the term *internal control*. For the purposes of Section 404, the great majority of companies and all the CPA firms[xiv] use the definition in COSO's *Internal Control — Integrated Framework*. COSO's definition relates to all aspects of internal control, not just that over financial reporting. The following is from the report's executive summary:

> "Internal control is broadly defined as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - effectiveness and efficiency of operations
> - reliability of financial reporting
> - compliance with applicable laws and regulations
>
> "The first category addresses an entity's basic business objectives, including performance and profitability goals and safeguarding of resources. The second relates to the preparation of reliable published financial statements, including interim and condensed financial statements and selected financial data derived from such statements, such as earnings releases, reported publicly. The third deals with complying with those laws and regulations to which the entity is subject. These distinct but overlapping categories address different needs and allow a directed focus to meet the separate needs."

KEY POINTS

COSO PRINCIPLES OF INTERNAL CONTROL

- *"Internal control is broadly defined as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives."*
- *"While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time."*

COSO goes on to say:

> "Internal control systems operate at different levels of effectiveness. Internal control can be judged effective in each of the three categories, respectively, if the board of directors and management have reasonable assurance that:
>
> - they understand the extent to which the entity's operations objectives are being achieved
> - published financial statements are being prepared reliably
> - applicable laws and regulations are being complied with

> "While internal control is a process, its effectiveness is a state or condition of the process at one or more points in time."

The PCAOB, together with the SEC, is responsible for the rules governing the roles and actions of the CPA firms. In AS 5, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements*, the PCAOB has a definition that is consistent with that of COSO, although limited to financial reporting. It is also consistent in all material respects with the definition used by the SEC.[xv] They define ICFR as:

> "A process designed by, or under the supervision of, the company's principal executive and principal financial officers, or persons performing similar functions, 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 for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:
>
> 1. Pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company;
> 2. Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and
> 3. 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."

There are a number of key points in these definitions:

1. Internal control is a *process*. It is a continuing process rather than a point-in-time situation. However, any assessment of its effectiveness is made at a point in time. Management must assess the adequacy of its ICFR as of year-end, even though the system operates continuously — not only all year but for multiple years. Management also needs to be aware, though, that an assessment as of a point in time is likely to be interpreted by investors and others as indicative of its continuing effectiveness. Stakeholders are concerned with whether or not the internal controls are sufficient to provide comfort, not only with respect to the reliability of the current set of financial statements but also of future financial statements.

KEY POINTS

REASONABLE ASSURANCE

- *"An internal control system, no matter how well conceived and operated, can provide only reasonable — not absolute — assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be fault, and that breakdowns can occur because of simple error or mistake."*

2. Internal control only provides *reasonable assurance*. The COSO executive summary expands on this point:

> "An internal control system, no matter how well conceived and operated, can provide only reasonable — not absolute — assurance to management and the board regarding achievement of an entity's objectives. The likelihood of achievement is affected by limitations inherent in all internal control systems. These include the realities that judgments in decision-making can be faulty, and that breakdowns can occur because of simple error or mistake.
>
> "Additionally, controls can be circumvented by the collusion of two or more people, and management has the ability to override the system. Another limiting factor is that the design of an internal control system must reflect the fact that there are resource constraints, and the benefits of controls must be considered relative to their costs."

In its guidance for management, the SEC states:

> "The 'reasonable assurance' referred to in the Commission's implementing rules relates to similar language in the Foreign Corrupt Practices Act of 1977 (FCPA). Exchange Act Section 13(b)(7) defines 'reasonable assurance' and 'reasonable detail' as 'such level of detail and degree of assurance as would 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 upon which an issuer may reasonably base its decisions."

An effective system of internal control can only provide this *reasonable assurance*. When assessing its adequacy, management needs to determine whether errors — even if they resulted in a material error in the financial statements — are the result of a "simple error or mistake" that is a momentary or one-time failure, rather than an indication that the system no longer provides *reasonable assurance* that a material error in the financials will not be prevented or detected. COSO, the PCAOB, and the SEC refer to the concept of a prudent official or reasonable person's view, which should be considered when determining whether the system of internal control provides reasonable assurance.

The PCAOB states that *reasonable* is a "high level of assurance." They refer to the "understanding that there is a *remote likelihood* [emphasis added] that material misstatements will not be prevented or detected on a timely basis." This is fully consistent with the way in which management and the external auditor should assess the overall system of internal control. As noted later, the external auditors typically use a range of 5 percent to 10 percent for remote likelihood.

The SEC has not provided a specific standard with which the effectiveness of internal control should be measured. Instead, in the words of their commentary on the final rules, they have set a "threshold for concluding that a company's internal control over financial reporting is effective." That threshold is the presence of one or more material weaknesses. Therefore, management can assess ICFR as effective if there are no control deficiencies such that a material error is reasonably possible.

Stating the issue more simply, a system of internal control provides a reasonable level of assurance with respect to filed financial statements (i.e., for Section 404) when:

- The cumulative risk of a material misstatement due to known control weakness is not reasonably possible (i.e., the likelihood is 10 percent or less).[1]
- Any control weaknesses identified by management and external or internal auditors are corrected promptly.
- The management team believes the level of controls is appropriate to the organization, enabling reliable financial reporting for external use (i.e., SEC filings).

3. Internal control over the integrity of a company's financial statements is part of the overall system of internal control. In practice, there can be significant overlap between controls designed to provide assurance over the financials and those that provide assurance relative to operational effectiveness or compliance. For example, monitoring the cost of units sold is an important control for both financial reporting and for ensuring the efficiency and effectiveness of operations. When assessing control deficiencies to determine the need and value of enhancing controls, management should consider the risk not only to the financial statements but also to the efficiency of operations or compliance with applicable rules and regulations.
4. Another point of significance is that for Section 404 purposes, ICFR only addresses the controls providing assurance over financial statements filed with the SEC. It does not necessarily address controls over:
    - Other financial statements, including those provided as part of statutory reporting to foreign governments or to financial institutions as may be required by debt instruments.
    - Financial reports used in internal management's decision making (e.g., monthly management metrics).
    - Other sections of the 10-K, such as Management's Discussion and Analysis (MD&A).
    - Earnings releases and proxy statements.

1 The 10-percent reference is based on the external auditors' general use of a range of 5 percent to 10 percent when determining whether the likelihood of a material error is 'more than remote.' While it is not generally possible to calculate the probability of an error with any degree of precision, and there is no authoritative guidance in this area, this range is helpful in providing management with a feel for the level of probability being discussed.

Clearly, management needs to have effective controls over all forms of financial reporting and may consider either extending its own assessment to cover these areas or asking its internal auditing function to perform procedures relative to these areas.

The COSO Framework

Management is required to assess its system of ICFR using a recognized framework. Most have selected the COSO framework, which is recognized as appropriate by the SEC and PCAOB.

COSO's internal control framework describes internal controls as consisting of five interrelated components. These are generally called "layers," and the controls within each must be included in management's assessment. The five layers are described by COSO as:

Control Environment. "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors."

Risk Assessment. "Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to achievement of the objectives, forming a basis for determining how the risks should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change."

Control Activities. "Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties."

Information and Communication. "Pertinent information must be identified, captured, and communicated in a form and time frame that enable people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to informed business decision making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization. All personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information

upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders."

Monitoring. "Internal control systems need to be monitored — a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Ongoing monitoring occurs in the course of operations. It includes regular management and supervisory activities and other actions personnel take in performing their duties. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and the effectiveness of ongoing monitoring procedures. Internal control deficiencies should be reported upstream, with serious matters reported to top management and the board."

In practice, the assessment of ICFR is conducted at two levels within the organization:

- **Entity-level** activities generally operate at a corporate level, and typical examples are corporate policies, the activities of the board of directors, and the period-ending financial close
- The **Activity Level** generally relates to individual business locations or business processes. Examples might include accounts payable, direct supervision of employees, and the hiring process for new employees.

Most of the controls that are assessed are located at the activity level. However, particular attention to entity-level controls is required because:

- These controls are presumed to have a pervasive effect on the activities of the entire company.
- Many of the control deficiencies underlying the more public accounting issues of the last several years, including Enron and WorldCom, were in these areas.
- Assessing entity-level controls early, if not first, can often affect the selection of controls to be tested at the activity level. For example, a review of month-to-month fluctuations in payroll costs that is performed as part of the financial period-end close may be sufficient in some companies to detect material errors arising from payroll processing. In that case, management may decide there is no need to perform additional testing within the payroll process itself.

It should be noted that activities in each of the five layers typically can be found at both the entity-level and the activity level. For example:

- *Control Environment* activities include the organization's code of conduct (an entity-level control) as well as employee candidate background checks (performed at the activity level).
- *Risk Assessment* includes assessing the risk of an unassertive audit committee (entity-level) or the existence of excess inventory.
- *Control Activities* include top-level reviews performed as part of the corporate close process (entity-level) as well as bank reconciliations (activity level).

- *Information and Communication* includes information on warranty claims used to calculate the warranty reserve as part of the financial close process (entity-level), and communicating to employees performance expectations (activity level).
- *Monitoring* includes the internal audit activity (entity-level), as well as the direct supervision of payroll staff (activity level).

A number of companies use a separate framework to supplement COSO when assessing IT controls. COBIT[xvi] was developed by the Information Systems Audit and Control Association's IT Governance Institute in 1994 and is widely used by IT audit professionals in the United States and overseas. Its fourth edition, which was released in December 2005, includes important updates for Section 404 and strengthens links to frameworks such as COSO. It was further updated by edition 4.1 in May 2007.

Additional information on internal controls may be obtained from the head of the internal audit function, The IIA, or the external auditor.

C. What Constitutes an Effective System of Internal Control as it Relates to the Requirements of Section 404?

Management needs to determine whether the system of internal control in effect as of the date of the assessment provides reasonable assurance that material errors, in either interim or annual financial statements, will be prevented or detected.

Management is able to make this assessment by:

1. Identifying, assessing, and testing the design and operating effectiveness of the key controls that will either prevent or detect material errors in the transactions that constitute the balances in significant accounts in the financial statements, or in the way the financial statements are prepared and presented.
2. Assessing whether any control deficiencies identified in the above process represent, either individually or in aggregate, a reasonable possibility of a material error (i.e., a material weakness).

> *If the scope and quality of management's identification, assessment, and testing of key controls is sufficient to address all major risks to the integrity of the financial statements and no material weaknesses are identified, then management will normally be able to assess the system of ICFR as effective. However, the presence of a single material weakness precludes management from making such an assessment. This is appropriate, as a material weakness by definition indicates that the system of internal control does not provide reasonable assurance regarding the reliability of the financial statements.*

Each of the above is discussed in more detail below.

D. Who Is Responsible for Internal Controls?

Sections 302 and 404 of Sarbanes-Oxley make it clear that management — specifically the CEO and CFO — is responsible for the adequacy of internal controls. The certification by these officers required by Section 302 states that:

> "(4) the signing officers —
>
> (A) are responsible for establishing and maintaining internal controls.
>
> (A) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared.
>
> (A) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report.
>
> (A) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date."

While the CEO and the executive team as a whole may look to the CFO for overall leadership and accountability for financial reporting, other parts of the organization have a significant part to play. For example, the system of ICFR typically includes processes in the procurement, inventory management, manufacturing, sales, and information technology functions, not all of which report to the CFO.

Responsibility for the system of internal control within a typical organization is a shared responsibility among all the executives, with leadership normally provided by the CFO.

The audit committee of the board of directors has a significant role in a company's system of internal control, which it performs on behalf of the full board and ultimately the shareholders. Specifically, the members:

- Provide oversight of management. Both management and the external auditor are required to consider the effectiveness of the audit committee as part of their assessments of ICFR. COSO describes their role:

  "Management is accountable to the board of directors, which provides governance, guidance, and oversight. Effective board members are objective, capable, and inquisitive. They also have a knowledge of the entity's activities and environment, and commit the time necessary to fulfill their board responsibilities. Management may be in a position

> to override controls and ignore or stifle communications from subordinates, enabling a dishonest management which intentionally misrepresents results to cover its tracks. A strong, active board, particularly when coupled with effective upward communications channels and capable financial, legal, and internal audit functions, is often best able to identify and correct such a problem."

- Provide direction and oversight of the work of the external auditor, who is appointed by and reports directly to the audit committee.
- Direct and oversee the performance of the internal auditing function, which typically reports to the audit committee.

The external auditor is engaged by and directly accountable to the audit committee, a requirement of Sarbanes-Oxley. Through their audit of the annual and review of the interim financial statements, and their audit of the system of internal control over financial reporting, they provide the audit committee, board of directors, investors, and management with assurance of the reliability of the financial statements. Although the external auditor provides assurance to the audit committee relative to the financial statements filed with the SEC, management is not permitted to place reliance on their work for purposes of Section 404. Instead, management must have a system of internal control that is sufficient without relying on the external auditor.

By contrast, the internal auditing function is considered part of an organization's internal control system, even though it also is directly accountable to the audit committee in most public companies. While the chief internal audit executive (CAE) may report to a senior executive for administrative matters, he or she should report functionally to the audit committee. The internal auditing function provides assurance to both management and the audit committee regarding the effectiveness of all aspects (i.e., not only financial, but also operational effectiveness and compliance) of an organization's system of internal control, risk management, and governance practices.[xvii] Its activities are considered part of the "monitoring" layer of the system of internal control and, therefore, are included in both management's and the external auditor's assessment. COSO describes their work:

> "Internal auditors play an important role in evaluating the effectiveness of control systems, and contribute to ongoing effectiveness. Because of organizational position and authority in an entity, an internal audit function often plays a significant monitoring role."

The audit committee can and should rely on the assurances of management, internal auditors, and the external auditor in forming their own assessments and in approving financial statements that are filed with the SEC. Additional information on the role and responsibilities of each participant can be obtained from the company's CAE or The IIA.

E. What Is the Scope of Management's Assessment of the System of Internal Control Over Financial Reporting?

Management is actually required to provide more than one assessment of internal controls in its filings with the SEC. One is required by Section 302 and is included in quarterly and annual financial reports, while the other is required by Section 404 and is only included in annual reports.

When the SEC developed the detailed rules for implementing Section 302,[xviii] it required the CEO and CFO to make a number of statements relative to internal controls (i.e., the Section 302 certification). The SEC also required companies to include in their annual and quarterly financial statements an assessment of its disclosure controls and procedures (i.e., disclosure controls), a new term not actually mentioned in Sarbanes-Oxley. The SEC defined disclosure controls as:

> "…controls and other procedures that are designed to ensure that information required to be disclosed by the company in its Exchange Act reports is recorded, processed, summarized, and reported within the time periods specified in the Commission's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by the company in its Exchange Act reports is accumulated and communicated to the company's management (including its principal executive and financial officers) for timely assessment and disclosure pursuant to the SEC's rules and regulations."

A simple and practical definition of the scope of Section 404 is that it addresses everything in the GAAP-based interim and annual financial statements and related notes that are filed with the SEC.[xix] Disclosure controls include this and more.

The scope of disclosure controls is broad, including all "information required to be disclosed by the company in its Exchange Act reports." These reports include not only the financial statements and related footnotes but nonfinancial information as well. It is important to note that disclosure controls cover not just the quarterly and annual financial statements filed on Forms 10-Q and 10-K but also notifications of material events filed on Form 8-K or other current reports.[xx] By contrast, Section 404 only relates to the financial information required to be included in filings with the SEC.

Disclosure controls include in their entirety all the Section 404 internal controls over financial reporting. Although the SEC in its early publications indicated that there would be significant overlap, in practice there are no key internal controls over financial reporting for Section 404 that are not part of disclosure controls.[xxi] On the other hand, there are significant areas covered under disclosure controls that are not part of ICFR. Examples of the latter include MD&A and the timely notification to investors using Form 8-K of material events.

Companies need not only (a) internal controls to ensure the completeness and accuracy of the financial information included in its filings with the SEC, but also (b) internal controls to ensure the completeness, accuracy, and timeliness of nonfinancial information filed with the SEC. The combination of the two represents ***disclosure controls****.*

As a result:

- The assessment of disclosure controls can be that they are not effective, even though internal controls are effective, for example due to issues surrounding the timely notification of material events to investors.
- If internal control over financial reporting is assessed as ineffective, disclosure controls cannot be considered effective.[1] This is because the financial information included in the filings with the SEC is the most critical part of those reports.

Section 302 requirements include, as mentioned above, a certification by the CEO and CFO and an assessment of its disclosure controls. The certification includes the following statements that relate to internal controls:

> "4. The registrant's other certifying officer and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a-15(e) and 15d-15(e)) and ICFR (as defined in Exchange Act Rules 13a-15(f) and 15d-15(f)) for the registrant and have:
>
> (a) Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;
>
> (b) Designed such internal control over financial reporting, or caused such ICFR to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;
>
> (c) Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of

1 Management may want to consult with SEC counsel on this matter. As discussed in note xiii, the SEC and certain SEC counsel believe (and we concur) there are aspects of ICFR that are not included in disclosure controls. However, we believe all key controls for Section 404 will be included. An analysis of filings with the SEC in year one of Section 404 identified that 94% of the companies that assessed their ICFR as ineffective also assessed their disclosure controls as ineffective.

the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

(d) Disclosed in this report any change in the registrant's ICFR that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and

"5. The registrant's other certifying officer and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

(a) All significant deficiencies and material weaknesses in the design or operation of ICFR which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

(b) Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting."

Clearly, there is a need to assess the adequacy of ICFR at interim periods to support the Section 302 certification, as well as the annual assessment required by Section 404.

There are some major differences between the annual Section 404 assessment and that required for the interim Section 302 assessments:

- The external auditors do not provide an interim assessment[xxii] for Section 302.
- There is no current requirement that the rigor and formality required in practice for Section 404 be repeated each quarter for the Section 302 assessment. For example, it is not required that management test all or even a significant portion of its key controls each quarter. In addition, management's Section 302 process is not required to follow a recognized internal controls framework.

However, prudence suggests that management:

- Has a reasonably formal, documented process for making the quarterly assessment that is included in the 10-Q and supports the Section 302 certifications.
  - We suggest that this can be included in the activities of the company's disclosure committee, which most of the larger companies have established.
  - The process should include the assessment of all internal control deficiencies known to management including those identified not only during management's assessment process but also by either the external auditor in their Section 404 work or by internal auditing in its various audit activities.

- As discussed below, the system of ICFR has to provide reasonable assurance with respect to the quarterly financial statements as well as the annual statements. The quarterly assessment is against a lower — typically one quarter the size — determination of what constitutes material.
- The process and results should be reviewed and discussed with the CEO and CFO to support their Section 302 certifications.

- Confirms that the external auditor does not disagree with management's quarterly assessment.
- Understands — which requires an appropriate process to gather the necessary information — whether there have been any major changes in the system of internal control during the quarter. A major change can include improvements and degradations in the system of internal control. While Section 302 only requires the disclosure in the 10-Q of a *material weakness* and the communication to the audit committee of a material or significant deficiency, the *correction* of a *significant* deficiency may be considered a major change and, if so, should be disclosed.

F. Defining the Detailed Scope for Section 404

Management's assessment for Section 404 is as of year-end, so there may be a temptation to wait until late in the year before starting the Section 404 program. However, there are important reasons for considering the program a continuous, year-round process and starting early each year:

- Significant resources are required for testing that may be in short supply later in the year. Testing can be performed throughout the year spreading the resource burden. Note: If controls are tested early in the year, management needs to perform an update procedure to "roll forward" the results to year-end.
- If there are issues relative either to the design or the consistent operation of the controls (i.e., exceptions will be identified during the testing), management will have time to make changes and retest successfully before year-end.
- The external auditors often have a policy requiring they start their testing only *after* management has tested and assessed the individual controls as effective. The earlier the external auditors perform their testing, the more time there is for management to remediate any issues and retest.

As explained above, spreading the testing provides management with improved assurance supporting the quarterly Section 302 certification and assessment of disclosure controls.

1) Using a Top-down and Risk-based Approach to Defining the Scope

In defining the detailed scope for management's assessment, a risk-based and top-down approach should be taken. As noted previously, the PCAOB requires such an approach in AS 5, and the SEC strongly recommends it in their guidance.

Both the PCAOB and the SEC's guidance provide principles-based guidance on the top-down approach, rather than a more prescriptive set of procedures.

AS 5 includes the following:

> "The auditor should use a top-down approach to the audit of internal control over financial reporting to select the controls to test. A top-down approach begins at the financial statement level and with the auditor's understanding of the overall risks to internal control over financial reporting. The auditor then 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 and related disclosures. The auditor then verifies his or her understanding of the risks in

the company's processes and selects for testing those controls that sufficiently address the assessed risk of misstatement to each relevant assertion.

"Note: 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 SEC uses different language, but the principles are the same:

"Management should evaluate whether it has implemented controls that will achieve the objective of ICFR (that is, to provide reasonable assurance regarding the reliability of financial reporting). The evaluation begins with the identification and assessment of the risks to reliable financial reporting (that is, materially accurate financial statements), including changes in those risks. Management then evaluates whether it has controls placed in operation (that is, in use) that are designed to adequately address those risks. Management ordinarily would consider the company's entity-level controls in both its assessment of risks and in identifying which controls adequately address the risks."

The SEC guidance continues with a high-level description of the steps involved:

- "Management should identify those risks of misstatement that could, individually or in combination with others, result in a material misstatement of the financial statements ("financial reporting risks"). Ordinarily, the identification of financial reporting risks begins with evaluating how the requirements of GAAP apply to the company's business, operations and transactions."
- "Management uses its knowledge and understanding of the business, and its organization, operations, and processes, to consider the sources and potential likelihood of misstatements in financial reporting elements. Internal and external risk factors that impact the business, including the nature and extent of any changes in those risks, may give rise to a risk of misstatement. Risks of misstatement may also arise from sources such as the initiation, authorization, processing, and recording of transactions and other adjustments that are reflected in financial reporting elements. Management may find it useful to consider "what could go wrong" within a financial reporting element in order to identify the sources and the potential likelihood of misstatements and identify those that could result in a material misstatement of the financial statements."
- "Management's evaluation of the risk of misstatement should include consideration of the vulnerability of the entity to fraudulent activity (for example, fraudulent financial reporting, misappropriation of assets, and corruption), and whether any such exposure could result in a material misstatement of the financial statements.

  "Management should recognize that the risk of material misstatement due to fraud ordinarily exists in any organization, regardless of size or type, and it may vary by specific location or segment and by individual financial reporting element. For example, one type of fraud risk

that has resulted in fraudulent financial reporting in companies of all sizes and types is the risk of improper override of internal controls in the financial reporting process."

- "Management should evaluate whether it has controls placed in operation (that is, in use) that adequately address the company's financial reporting risks. The determination of whether an individual control, or a combination of controls, adequately addresses a financial reporting risk involves judgments about whether the controls, if operating properly, can effectively prevent or detect misstatements that could result in material misstatements in the financial statements.

  "Management may identify preventive controls, detective controls, or a combination of both, as adequately addressing financial reporting risks. There might be more than one control that addresses the financial reporting risks for a financial reporting element; conversely, one control might address the risks of more than one financial reporting element. It is not necessary to identify all controls that may exist or identify redundant controls, unless redundancy itself is required to address the financial reporting risks."

- "In addition to identifying controls that address the financial reporting risks of individual financial reporting elements, management also evaluates whether it has controls over the period-end financial reporting process, controls in place to address the entity-level, and other pervasive elements of ICFR that its chosen control framework prescribes as necessary for an effective system of internal control. This would ordinarily include, for example, considering how and whether controls related to the control environment, controls over management override, the entity-level risk assessment process and monitoring activities, and the policies that address significant business control and risk management practices are adequate for purposes of an effective system of internal control."

2) The Detailed Process for Defining the Scope

Our suggested process, shown below, is consistent with the principles discussed above. It provides more detail than the SEC or PCAOB guidance, while remaining principles-based. It involves identifying:

- The general ledger accounts that make up each line in the financial statements as filed. For example, accounts payable is normally a single line in the financial statements, although it represents a group of related general ledger accounts.
- For each of the above, which accounts are considered significant.
- The financial statement assertions that are relevant to those accounts and material to the investor.
- The locations to include in scope.
- The business processes that process transactions into the significant accounts at in-scope locations.
- The key transactions representing balances in the above accounts.

- The key controls over those transactions that ensure the financial statement assertions are achieved.

Since so much will depend on whether the system of internal control provides reasonable assurance that a material error will be either prevented or detected, the place to start is a definition of *material error*, or the level of *materiality*.

3) Materiality

There is guidance in the accounting and auditing literature on this topic that is lengthy (and not repeated here), but comes down to a fairly simple test: what would be material to the reasonable investor when making an investment decision in the company's securities. Usually, this is 5 percent of the company's pre-tax net income, but may be different when the company has losses or low profit levels; both quantitative and qualitative aspects must be considered.

It is preferable if the external auditor agrees with management's determination of materiality, so early discussions should be held. The external auditor may indicate that only a preliminary determination may be made, as facts may change before the end of the year.

The determination of materiality for Section 404 should consider:

- The level of error that would be material to the full year's results if it affects the income statement.[xxiii]
- Not all errors affect the P&L, only the balance sheet. In a few cases, the errors are in the disclosures (e.g., footnotes or earnings per share calculations). These errors will have to be assessed on their specific facts and circumstances.
- In all cases, a bright-line definition must be tempered with an assessment of what a reasonable investor might conclude. It is easy to rush to judgment and label an error material that would have no effect on any investor's assessment of the company.

This determination of what would be material for the annual financials should be made by technical accounting personnel after discussion with the external auditors. The determination needs to consider both quantitative and qualitative factors.

Management should work closely with the external auditor at every stage of their Section 404 process, and materiality is an important agreement to make. Management's level should influence the external auditor's own level, which can have implications on the extent of testing and costs (both for management testing and external auditor fees).

KEY POINTS

WORKING WITH EXTERNAL AUDITORS

- *Management should work closely with the external auditor at every stage of their Section 404 process.*
- *Management's materiality will influence the external auditor's own level, which can have implications on the extent of testing and related costs.*

4) Significant Accounts and Disclosures

Having decided on a materiality level for the full year's P&L, management needs to determine how and where an error could occur. The financial statements are

examined to determine in which accounts and disclosures there is the possibility of a material error. These are considered "significant accounts."[1]

It should be noted that the SEC guidance does not include, as a step, the identification of significant accounts or locations, business processes, or major classes of transactions. Instead, it suggests that management identify financial reporting risks and the controls required to address those risks. The steps discussed here provide a process for identifying the risk of material misstatement of the financials (i.e., financial reporting risks) and related key controls.

Any account that is larger than the materiality level should be given strong consideration as a significant account, as there is at least a possibility that it could contain a misstatement that would be material to the financial statements. Management should also take into account the possibility that account balances will be higher at year-end (e.g., reflecting planned revenue growth).

Accounts that are small and highly unlikely to contain an error of a material amount can be excluded from the scope for Section 404. AS 5 advises that "the maximum amount that an account balance or total of transactions can be overstated is generally the recorded amount, while understatements could be larger." Absent qualitative factors (e.g., whether the account balance fluctuates significantly from period to period, or involves complex accounting with a significant level of judgment), accounts with balances less than the materiality level can generally be excluded from scope as being unlikely to contain a material error.[xxiv]

An important exception is where multiple small accounts are subject to a single point of failure and as a group exceed the materiality level. For example, a company may have multiple accounts for travel and entertainment expense (e.g., for hotel, meals, airfare, and other travel costs). However, it may use the same process for all travel and entertainment expense, and a failure in a single control could affect all travel and entertainment expense. In this case, management should group these related accounts and consider them all as significant.

The risk that multiple accounts are subject to a single point of failure is not uncommon. Other examples may include: manufacturing variance accounts, multiple accounts for fixed assets or inventory, different accounts for payroll benefits, and separate accounts for various types of supplies. Some external audit firms allow for this by lowering their materiality level for the selection of significant accounts. Management may follow the same approach or use its knowledge of the organization's processes and controls to include this consideration as a qualitative risk factor in the selection of significant accounts.

The grouping of accounts can also work to reduce the number of significant accounts. For example, fixed assets and accumulated depreciation may individually exceed the materiality level. However, they are reported together in the financial statements and management may determine that the risk of a material misstatement of net fixed assets is unlikely. A similar situation may occur with other accounts that tend to offset when combined for financial reporting purposes (e.g., intangibles and related amortization).

1 AS 5 describes significant accounts and disclosures as having "a reasonable possibility of containing misstatements that would cause the financial statements to be materially misstated."

The scope of Section 404 extends to the notes and other disclosures that are part of the financial statements. Management needs to perform a risk assessment on all of the notes to determine which are significant and the nature and magnitude of an error that would be considered material to the investor. That determination may affect the selection of which accounts to include in scope, perhaps including some accounts that are below the agreed materiality.

Materiality and the accounts in scope should be assessed at least quarterly, or when there are material changes in the business, to ensure there is no need to add or remove areas from scope.

5) Financial Statement Assertions

The external audit profession has identified a number of financial statement assertions that may be applicable to the selected general ledger accounts. AS 5 requires the external auditor to determine which of these are *relevant* (i.e., a potential source of misstatement). Management may decide to follow the same process and ensure all relevant assertions for each significant account are addressed by appropriate key controls. The assertions suggested by AS 5 are as follows:

- **Existence or Occurrence** addresses whether assets or liabilities exist at a given date and whether recorded transactions have occurred during a given period.
- **Completeness** addresses whether all transactions and accounts that should be presented in the financial statements are so included.
- **Valuation or Allocation** addresses whether asset, liability, equity, revenue, and expense components are included in the financial statements at appropriate amounts.
- **Rights and Obligations** relates to whether the rights and liabilities are the obligations of the entity at a given date.
- **Presentation and Disclosure** addresses whether particular components of the financial statements are properly classified, described, and disclosed.

6) Significant Locations, Business Processes, and Major Classes of Transactions

The majority of companies have operations in multiple locations, and an analysis should be performed to identify those locations that are *significant*. It should be performed separately for each significant account, as follows:

- For each significant account, identify those locations whose transactions are involved.
- Determine whether there is at least a reasonable possibility of a material error resulting from that location's transactions in the significant account. If so, that location is significant for that account.
- For locations that are not significant for an account, assess whether there are multiple locations that should be aggregated for risk assessment purposes. For example, if transactions for several locations share a common process and rely on the same control, the failure of that common control could result in misstatements in multiple locations that are individually not material, but that are material in the aggregate.

AS 5 includes a short but useful paragraph of guidance.[xxv]

> "In determining the locations or business units at which to perform tests of controls, the auditor should assess the risk of material 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.
>
> "Note: The auditor may eliminate from further consideration locations or business units that, individually or when aggregated with others, do not present a reasonable possibility of material misstatement to the company's consolidated financial statements."

The balances in the significant accounts are the result of transactions that flow through a number of business processes. For each significant account and location combination, the key business processes now need to be identified.[xxvi]

We recommend identifying which transactions make up the preponderance of the account balances and which represent a reasonably possible source of material misstatement. That will enable a focus on those material transactions together with the related processes and controls, and the exclusion of immaterial transactions that flow into significant accounts. For example, the significant account for depreciation may include not only the depreciation of plant and equipment, but also the depreciation of company vehicles. For most companies, depreciation of the small number of company vehicles is not material either to the P&L or the balance sheet and should be excluded from Section 404 scope.

At this point, management has defined materiality and identified:

- The significant general ledger accounts and notes to be included in scope.
- At which locations the controls and processes related to those accounts will be assessed and tested.
- The business processes and material transactions that make up the balances in those accounts.

7) Key Control

Although referenced in some PCAOB documents, including the Nov. 30, 2005 report, there is no commonly accepted definition of a key control. We support the following, which we believe is consistent with PCAOB and SEC published guidance:

> *A key control is a control that, if it fails, means there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis. In other words, a key control is one that is required to provide reasonable assurance that material errors will be prevented or timely detected.*

Careful identification of key controls is important to an efficient and effective Section 404 program. An overly conservative approach, where too many controls are defined as *key*, will result in excessive time and resources testing controls that are not critical to the assessment.

It is important to note that there is no generic "laundry list" of what will always be considered a key control and, due to differences in systems, procedures, business environments and models, sound professional judgment is required during the identification process. Management should also give due consideration to the views of the external auditor and ensure they are comfortable with the process management uses for identifying key controls.

Controls may either prevent errors or detect their occurrence. Some experts include the determination of whether controls are preventive or detective in their process to identify key controls, because preventive controls are seen as stronger. However, management should recognize that an efficient and effective system of controls will use a combination of both, and we do not consider it critical to focus on whether controls are one or the other. Rather, management should focus on whether the controls in place are sufficient to ensure there are no misstatements of the financials and are appropriate in terms of management of business risk.

The identification of key controls should take into account the risk of fraud, including the override by management of controls. It is important to remember that while the prevention of fraud (or at least its detection) is important to the business, only the risk of fraud that results in a material misstatement of the financials must to be included in the Section 404 assessment (see the Fraud Risk Assessment section later in the guide).

The SEC's and PCAOB's guidance describes the top-down approach in a way that implies that entity-level controls should be understood and considered first, before understanding business process controls (at the activity level). However, AS 5 points out 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."

We believe that the controls that should be considered first are those that meet the definition of a key control (as described above). They have a direct effect on the risk of material misstatement, and may operate within business processes at either the entity-level (e.g., as part of the corporate financial close process) or the activity level (e.g., within a local accounts payable function).

Once the key controls have been identified, additional entity-level controls that have an indirect effect on the risk of material misstatement should be considered.

a. Identifying Key Controls Within Business Processes

There are two schools of thought when it comes to identifying key controls, both of which are discussed further below.

i. In the first, risks are listed that may prevent the financial assertions from being satisfied. Then, the controls that address those risks are identified. The benefit of this approach is that it is relatively straight forward, familiar to most experienced auditors, and suggested in the SEC guidance. However, the risk of this approach is that the list of risks may not be complete.

The majority of companies use this alternative, which starts with the significant general ledger accounts by location, defines the relevant financial assertions for each, and then lists all the risks to achievement of the assertions. Finally, the key controls are identified: those required to address each risk such that a material error is not likely. For example, the process may start with cash at the headquarters location and identify existence as one of the assertions to be achieved. The bank reconciliation is identified as the key control that addresses that assertion.

It is important to ensure the list of risks is complete. The external auditor may have a list of standard or common risks for different types of accounts, and the internal auditor can assist with a review of the list of risks. An additional source, if the company uses specialized Section 404 software, is the vendor of the software who typically has templates that management may use.

ii. By way of contrast, the second approach looks at the material transactions that flow into the significant accounts and identifies the controls that assure they are completely and accurately processed and recorded, and that only valid transactions are processed. The second approach, which has been adopted less frequently, includes controls that assure the safeguarding and existence of the assets and the presentation of account balances in the financial statements. The benefit of the second approach is that it provides more assurance that all the controls are addressed; however, it is more complex.

Both approaches have merit. Management should make a choice based on which is more consistent with the experience and training of the individuals managing the project, after consultation with the external auditor.

Whichever approach is taken, the process of identifying key controls should be top-down. When identifying key controls, it is important to recognize that sometimes several controls are required to work as a combination to provide assurance. The controls may operate at the same level (e.g., at the activity level, such as the preparation of a bank reconciliation by a staff member and its separate review and approval by a manager) or function at different levels (e.g., at the entity and activity levels, such as the posting of a journal entry by the controller at a division and a review by the corporate controller during the period-end close to ensure all major journal entries were posted).

- The selection should start by assessing whether there are any key controls operating at the entity-level that would be sufficient to prevent or detect a material misstatement relating to a significant account at a significant location. When such controls exist and are effective, management may determine there is no need to identify controls at lower levels. AS 5 explains this situation:

  > "Some entity-level controls might be designed to operate at a level of precision that would adequately prevent or detect on a timely basis misstatements to one or more relevant assertions. If an entity-level control sufficiently addresses the assessed

risk of misstatement, the auditor need not test additional controls relating to that risk."

An example of this situation might be the controls over payroll expense at a manufacturing company. If headcount is relatively stable and fluctuations are well below materiality levels, a high-level review performed as part of the period-end close process might be sufficient to detect any significant error. In that case, activity-level controls, such as those within the payroll business process over adding employees to payroll and changing salary and deduction information, probably will not need to be tested as key controls.

It should be noted that high-level reviews such as this are not necessarily performed at the company- or entity-level. They may be performed at the location itself, a regional headquarters, a shared service center, or at the corporate level.

- The next step is to determine whether there are detective controls, similar to entity-level controls but operating at an *intermediate level* (e.g., regional, shared service center, or local management level), that provide reasonable assurance that material errors would be detected on a timely basis.

  As with entity-level controls, effective intermediate-level controls may be sufficient by themselves, and controls within the activity not included as key controls.

- If insufficient controls are identified at higher levels, *activity level controls* should be reviewed and key controls identified.

Key controls, regardless of the level at which they operate (e.g., entity, intermediate, or activity) vary in how they work.

- Some controls are fully manual, such as the inspection of incoming materials for quality.
- Some key business controls are fully automated, for example the calculation of interest for banks or updating the correct general ledger account.
- Some controls are partly automated — also known as *hybrid* controls. For most companies, a large number of controls are of this type, where the individual performing the control relies on a report from the organization's primary business application, a data warehouse, or information on a computer screen. An example of this is the bank reconciliation, where the control uses reports from the general ledger system listing the cash balance and the various transactions that took place during the month. The reconciliation to the bank statement provides assurance that the reports are correct.

  Hybrid controls need to be examined carefully. If the normal operation of the manual portion of the control is sufficient to detect an error in the automated part (e.g., the computer report), then the control can be considered entirely manual since no reliance is being placed on the computer system. For example, the bank reconciliation might use a report from the general ledger system of cash transactions; if the report was incorrect or incomplete, it would be detected by the bank reconciliation process.

However, if the automated part of the control is not assured by the manual part, then it will have to be tested as an automated control. An example of a report that requires further testing is a report of all transactions over a defined dollar limit. The individual reviewing and taking action on this report cannot know that the report is complete and lists all items over the threshold. Therefore, the report should be tested as an automated control.

Key controls using a form of user computing, such as spreadsheets, may require special attention as described below.[1]

Some organizations have separated the identification of manual and automated controls, with the finance function (or financial internal auditors) identifying the manual controls and the IT function (or IT auditors) identifying the automated controls. This approach is likely to lead to significant problems because it is not top-down. Instead, the identification of IT controls — both automated controls within business processes and IT general controls (ITGCs) — should be the result of a top-down approach. The team performing the identification should have a solid understanding of the financial statements, business processes, and IT.

Segregation of duties (SOD) and restricted access (RA) controls need to be identified, assessed, and tested where they are key controls. Key SOD and RA controls include those that:

- Are required for an authorization control to be effective. For example, if the business control requires that all purchase orders be approved in the system by the purchasing manager, it is critical to ensure that only the purchasing manager has that capability.
- Reduce the risk of a material fraud that could be reported incorrectly in the financial statements (see (f) below).

With restricted access and segregation of duties, there is a risk of doing more work than is required for Section 404. While there are excellent business reasons for restricting access to only those functions individuals need to perform their assigned tasks, it is important to remember that only fraud risk that is both material and also misstated in the financials is within scope for Section 404. See the Fraud Risk section below.

b. Identifying Key ITGCs

When there is reliance on key automated controls, or on hybrid controls where failures in the automated part of the control might not be detected by the manual part, an assessment should be made to determine risks within ITGC processes and identify key ITGCs.

1 Note: some of the external audit firms emphasize a concept called key reports, which are commonly described as reports used in key controls. However, we believe the only key reports that need to be examined as automated controls are those where an error would not be detected in the normal course of the manual part of the control.

Broadly speaking, ITGC provide assurance that applications are developed and subsequently maintained, such that they provide the functionality required to process transactions and provide automated controls. They also assure the proper operation of the applications and the protection of both data and programs from unauthorized change.

The challenge to identifying key controls within ITGC is that they do not have a direct effect on the financial statements. Because ITGCs provide assurance on the continued, proper operation of key automated controls, a failure in a key ITGC control implies the loss of that assurance. In other words, reliance on ITGC is indirect — through reliance on key automated controls. If ITGC key controls fail, key automated controls may not be reliable; if they are not reliable, they might fail to perform their function of preventing or detecting a material error.

A key ITGC control meets the definition of a key control provided earlier: "A key control is a control that, if it fails, means there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis. In other words, a key control is one that is required to provide reasonable assurance that material errors will be prevented or timely detected." The difference is that the risk is indirect, through a lack of assurance over a key automated control.

A control within ITGC is, therefore, only key if it is linked to an identified key automated control. Otherwise, failures in the ITGC control would not result in the failure of a key automated control and, therefore, not represent a risk of material error in the financial statements.

The SEC guidance reinforces this:

> "For purposes of the evaluation of ICFR, management only needs to evaluate those IT general controls that are necessary for the proper and consistent operation of other controls designed to adequately address financial reporting risks."

Key controls in ITGC are, as a result, best identified through a continuation of the top-down and risk-based approach described here and in SEC and PCAOB guidance. The top-down approach identifies all the key automated controls that will be relied on. The top-down approach continues by identifying risks within ITGC processes (e.g., change management, security, or operations) to those key automated controls, and then the key controls within the ITGC processes necessary to address those risks. To quote the SEC again:

> "The identification of risks and controls within IT should not be a separate evaluation. Instead, it should be an integral part of management's top-down, risk-based approach to identifying risks and controls and in determining evidential matter necessary to support the assessment."

The IIA has published a Methodology (GAIT[xxvii]) that provides detailed guidance on how risks should be identified as a continuation of the top-down approach, as presented in this document. GAIT is consistent with the PCAOB's and SEC's guidance and has been adopted by a growing

number of organizations and their external auditors. The following discussion is based on the Methodology, which should be referenced for more detailed guidance.

Failure to define the scope of ITGC carefully can result not only in too much work (by testing controls that are not really key), but also in failing to address all the risks to key automated controls. In addition, ITGC processes can be extensive and include a significant number of controls relative to the development, maintenance, and operation of applications and infrastructure (e.g., operating systems and databases), as well as the security of the computer network, applications, and data. Due to the technical nature of ITGCs and the changing threats to network security, it is difficult for IT management to design and operate controls that are fully effective. As a result, IT management in many organizations has incurred significant costs, including personnel and software, to ensure ITGCs are adequately designed and operated. If the scope of ITGC that is relied upon for Section 404 is too broad, the assessment cost can be significant.

We recommend that management use the following process for identifying key controls within ITGC processes:

1. *Identify, and validate if necessary, critical IT functionality.*

   Critical IT functionality[xxviii] refers to functions performed by application software that must function consistently and appropriately if material errors are to be prevented or detected. They include:

   - Automated controls.
   - The automated portion of hybrid controls.
   - Other functionality that is not technically a control, but is necessary. Examples include complex calculations in a manufacturing company's warranty reserve, the aging of an accounts receivable report, the protection of information used in preparing the financial statements (i.e., data security), or the updating of transactions to the general ledger.

   In this step, a careful review is performed to ensure all the critical functionality has been identified. Experience shows that while automated controls are easy to identify, the other two may not be. In addition, this is an opportunity to confirm that there isn't any unnecessary duplication of coverage between multiple controls, including situations where both manual and automated controls provide sufficient assurance. In these cases, management can select which key controls will be tested and included in scope.

2. *Identify the significant applications where ITGCs need to be tested.*

   Significant applications are those where there is critical IT functionality. While there may be risk to business operations if ITGCs relating to other applications fail, because these other applications do not have any critical IT functionality, ITGC failures would not result in a material error in the financial statements.

Step 1 resulted in a list of all the critical IT functionality. The list is now sorted to identify the significant applications.

3. Identify ITGC process risks and related control objectives.

For each significant application, the ITGC processes (e.g., change management, security, and operations) need to be examined for risks. If a failure in one of those processes would be at least reasonably likely to result in a failure of a critical IT functionality, then the related IT control objectives need to be identified (e.g., all application code changes are approved).

Each organization will identify risks and related control objectives specific to their own facts and circumstances, since they depend on what they identify as critical IT functionality.

Examples of ITGC process risks and related IT control objectives are shown below:

- In a manufacturing company, a key automated control is the three-way match between purchase orders, records of goods received, and the vendors' invoices. The significant application containing this critical IT functionality is the company's SAP financial system. Using the GAIT Methodology, management determines that a failure to properly approve, test, and make changes to the code might result in a failure of the three-way match to operate appropriately. Then, the IT control objectives are identified: (a) "all changes to the SAP financial system are properly approved;" (b) "all changes to the SAP financial system are adequately tested;" and (c) "changes to the SAP financial system are accurately placed into production."
- An insurance company relies on historical records of claims received in the calculation of reserves. It determines that inappropriate changes to that data might result in errors in the reserve calculation that would not be detected. Protection of the data is seen as critical IT functionality; the risk is that the data might be changed, and the IT control objective is that "only approved changes are made to the historical record of claims."

Additional details on how to perform this step can be found in the GAIT Methodology.

4. Identify the ITGC to test that it meets control objectives.

Key controls are identified that will achieve each of the IT control objectives. That may require one or a number of related key controls, which operate within ITGC processes.

It should be noted that, in some organizations, ITGC processes may reside outside the IT function. For example, some technology companies may delegate management of the security of part of the network to the product development function, and other companies may have management of data warehouses (including security and application change control) within the finance organization.

5. Perform a "reasonable person" review.

The identification of key controls within ITGC can be complex, especially the first time it is done. We recommend that management take the opportunity to "step back" and review the

selection to determine whether a reasonable person, also known as a prudent official, would consider the selection of key controls to be appropriate.

This is also the time to determine whether there are any risks within ITGC processes that should be addressed because they affect multiple applications and their functionality. This *aggregation* effect is important. Many, but not all, ITGC processes relate to multiple applications. While a failure in an ITGC process might not represent a significant risk to an individual application and its critical functionality, the combined effect on multiple applications might be sufficient to justify testing related key controls.

c. Other Entity-level Controls

In addition to entity-level controls that have a *direct* relationship to the risk of material misstatement (e.g., high-level reviews during the corporate close process), there are other entity-level controls that only have an *indirect* relationship.

The SEC guidance describes entity-level controls:

> "The term 'entity-level controls' … describes aspects of a system of internal control that have a pervasive effect on the entity's system of internal control such as controls related to the control environment (for example, management's philosophy and operating style, integrity and ethical values; board or audit committee oversight; and assignment of authority and responsibility); controls over management override; the company's risk assessment process; centralized processing and controls, including shared service environments; controls to monitor results of operations; controls to monitor other controls, including activities of the internal audit function, the audit committee, and self-assessment programs; controls over the period-end financial reporting process; and policies that address significant business control and risk management practices. The terms 'company-level' and 'entity-wide' are also commonly used to describe these controls."

In the paragraph above, the following generally have a direct relationship to the risk of financial misstatement: controls over management override; centralized processing and controls; controls to monitor results of operations; many of the controls to monitor other controls; and controls over the period-end financial reporting process. Reliance on these controls would be identified in section b above. However, the following only have an indirect relationship: management's tone at the top; code of ethics; board or audit committee oversight; the risk management process; and the activities of the internal auditing function.

Management and the external auditor may decide to take different approaches to assessing and testing the indirect entity-level controls. The external auditor is directed in AS 5 to review many of these controls since poor controls could indicate a greater risk that the key controls are ineffective:

> "The auditor must test those entity-level controls that are important to the auditor's conclusion about whether the company has effective internal control over financial reporting. The auditor's evaluation of entity-level controls can result in increasing

or decreasing the testing that the auditor otherwise would have performed on other controls."

"Entity-level controls vary in nature and precision —

- Some entity-level 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.
- Some entity-level controls monitor the effectiveness of other controls. Such controls might be designed to identify possible breakdowns in lower-level controls, but not at a level of precision that would, by themselves, sufficiently address the assessed risk that misstatements to a relevant assertion will be prevented or detected on a timely basis. These controls, when operating effectively, might allow the auditor to reduce the testing of other controls.
- Some entity-level controls might be designed to operate at a level of precision that would adequately prevent or detect on a timely basis misstatements to one or more relevant assertions. If an entity-level control sufficiently addresses the assessed risk of misstatement, the auditor need not test additional controls relating to that risk."

AS 5 continues:

"*Control Environment*. Because of its importance to effective internal control over financial reporting, the auditor must evaluate the control environment at the company. As part of evaluating the control environment, the auditor should assess —

- Whether management's philosophy and operating style promote effective internal control over financial reporting;
- Whether sound integrity and ethical values, particularly of top management, are developed and understood; and
- Whether the Board or audit committee understands and exercises oversight responsibility over financial reporting and internal control."

The external auditor is also told they "must evaluate the period-end financial reporting process." However, the controls within the period-ending financial reporting process are generally direct controls that are separately identified by the top-down approach described earlier.

The contrast with the guidance for management from the SEC is significant. The SEC asks management to use the adopted internal controls framework (e.g., COSO) to determine how much work should be done on the indirect entity-level controls:

"In addition to identifying controls that address the financial reporting risks of individual financial reporting elements, management also evaluates whether it has controls over the period-end financial reporting process, controls in place to address the entity-level and

other pervasive elements of ICFR that its chosen control framework prescribes as necessary for an effective system of internal control. This would ordinarily include, for example, considering how and whether controls related to the control environment, controls over management override, the entity-level risk assessment process and monitoring activities, and the policies that address significant business control and risk management practices are adequate for purposes of an effective system of internal control. The control frameworks and related guidance may be useful tools for evaluating the adequacy of these elements of ICFR."

We agree in principle with the SEC's guidance. Management should assess those controls that are relevant to assessing that a reasonable system of internal control is in place. If the COSO framework has been adopted, we suggest reviewing and testing as appropriate key controls over:

- The risk of management override of key controls, accounting, or reporting.
- The provision of sufficient, skilled, and experienced staff in key positions.
- Management's assessment of the risks to financial reporting and the actions they take to manage those risks.
- The board and management's tone at the top, including the adequacy of the organization's codes of conduct.

The external auditor may be able to rely on portions of management's testing on these entity-level controls, so coordination to synchronize approaches and scope may be of value.

d. Spreadsheets and Other End-user Computing Issues

Much has been made about the risks to financial reporting through errors in spreadsheets and user computing in general, including the use of Microsoft Access databases and Business Objects reporting. Because spreadsheet errors have been found at a number of companies and resulted in material errors in their financial statements, this risk needs to be acknowledged and addressed.

KEY POINTS

SPREADSHEETS

- *If an error in the spreadsheet would not be detected in the normal operation of the control, understand where the risk is and take action accordingly.*
- *If a walk-through or other formal assessment of the control design is performed, it should include a discussion of how the completeness and accuracy of the spreadsheet results are assured.*

Risks related to spreadsheets (from here on, the term *spreadsheets* is used to include other end-user software) include:

1. Errors in the download from the company's systems such as:
   a. An incomplete download (e.g., missing a G/L or a region).
   b. An out-of-date download.
   c. A partial download, where transmission or

other errors prevented completion of the entire download.

d. Use of an intermediate database (e.g., a data warehouse) that is not complete, accurate, or current.

e. The incorrect population of the download data into the various cells in the spreadsheet.

2. Errors in spreadsheet calculations, sorts, or other programmable elements.

3. Use of an out-of-date spreadsheet, including use of a current spreadsheet where the calculations are not refreshed.

4. Changes to the data by the user.

5. Errors in the understanding or use of the spreadsheet (e.g., where the user is not the developer and picks up the wrong total).

6. Changes to the spreadsheet by another user due to poor security controls.

Some consultants have advised the use of specialized software in this area, and there are many products of value. However, before acquiring and implementing additional products, we recommend management consider the following approach:

- When a key business control includes the use of a spreadsheet, determine whether an undetected error in the spreadsheet could cause the control to fail and result in a material error in the financial statements. Also, determine whether the spreadsheet is essential to the key control (e.g., enabling a review of an estimate) or incidental (e.g., used to list the documents being reviewed).
- Will the normal operation of the control detect an error in the spreadsheet? There are two ways this can happen:
  - If the spreadsheet is used in a reconciliation process. For example, if original documents are summarized in a spreadsheet and compared to the updated general ledger balance, an error in the spreadsheet will result in an out-of-balance condition with the general ledger.
  - The control includes user procedures to confirm the completeness and accuracy of the spreadsheet. For example, if a spreadsheet is used to analyze sales invoices by region, then confirmation of the totals to the general ledger will ensure that the download of data into the spreadsheet is complete and formulas are properly calculating the totals.
- If an error in the spreadsheet would not be detected in the normal operation of the control, understand the risk and take action accordingly:
  - If the risk is in the download from the general ledger (or other computer system) directly into the spreadsheet, consider changing the design of the control to include a user control (e.g., a user verification of the spreadsheet totals to the general ledger).

- If the risk is around the download of information into a data warehouse or similar (e.g., Essbase or Hyperion), consider adding controls over the download and ensuring that the spreadsheet is balanced back to the data warehouse.
- If the issue is that the user is entering data into the spreadsheet manually, consider adding a control to validate the completeness and accuracy of the data in the spreadsheet.
- If the risk of error is in the calculations, consider whether the user can review the results in such a way that it will confirm the calculations are correct. If the calculations are too complex for a review, consider replacing the spreadsheet with a report or other program developed and maintained by IT. A risk of using complex calculations in a spreadsheet is that the user may inadvertently introduce a mistake into the spreadsheet. Converting the spreadsheet into a report developed and maintained by IT will provide greater assurance that the calculations will continue to function properly, with all changes to the calculations tested and approved, assuming that IT has adequate ITGCs.
- If there is no alternative to relying on the spreadsheet and its calculations, ensure there are controls similar to those discussed in ITGC over:
  - The validity of changes to the spreadsheet, including testing and approval.
  - Input, whether automated or manual, of data into the spreadsheet.
  - The security of the spreadsheet, so that only valid, tested, and approved changes are made and that data is not inappropriately changed.
  - The way in which the spreadsheet is used and the results are interpreted. For example, there should be controls to ensure that all data is input and validated before the results of the spreadsheet are used in the key controls. In addition, there should be assurance (e.g., through documentation or user instructions) that the use of the spreadsheet is correct (e.g., the correct totals are used). An example of the latter is where a spreadsheet has multiple analyses of the data; the user should understand which analysis and which totals should be used.

When reviewing and assessing the adequacy of the design of key controls using one or more spreadsheets, the above should be considered. If a walkthrough or other formal assessment of the control design is performed, it should include a discussion of how the completeness and accuracy of the spreadsheet results are assured.

To assist the external auditor's review, as well as a solid double-check in this area, management should consider developing an inventory of all spreadsheets that are a significant part of a key control or a critical part of the financial reporting process. The inventory should describe how assurance is obtained for the completeness and accuracy of each spreadsheet, while testing of key controls should encompass the controls over the completeness and accuracy of the spreadsheet.

Where the spreadsheet is not assured by the normal operation of the control, management should consider performing periodic independent tests of the spreadsheet. For example, they may be included in the population of automated controls tested by IT auditors.

e. Controls Performed by Third-party Organizations (SAS 70 Type II Reports)

Many companies have achieved cost savings or other benefits by outsourcing selected functions, such as payroll processing, processing of stock options, or data center management. Management needs to consider these outsourced operations when developing the scope of the Section 404 assessment.[xxix] If key controls are operated by third-party organizations, they need to be assessed and tested before management can be assured that the controls are adequately designed and operating effectively.

One approach is to treat processes and related controls in the same way as management addresses processes and controls within the organization. Management needs to ensure the processes are adequately documented, identify and assess the adequacy of the design of key controls, and perform tests to confirm the controls are operating effectively and are consistent with the documentation. Management may find that the service provider has good documentation, in which case it need not duplicate that effort, even if the provider's documentation is not in the same format or style as that used by the company. Management may also be able to place some degree of reliance on any testing by the provider of its internal controls. However, management needs to consider not only the competence of the personnel performing such testing, but also the independence of the personnel from the provider's management.

Most service providers in the United States recognize their customers' need to obtain assurance over their provider's controls. Rather than have every customer send a team of auditors to document and test their controls, these providers engage a third-party auditor to perform an attest engagement under the AICPA's Statement of Auditing Standards Number 70 (SAS 70). This standard defines how independent auditors identify the controls to test, perform testing of the controls, and report the results. Reports from audits performed by independent audit firms in accordance with the provisions in SAS 70 — as long as the report is what the standard calls a type II report (some providers only obtain a type I report, which is not sufficient for Section 404) — can be relied upon by management as assurance that the providers' controls are adequate under certain conditions:

a) Management needs to identify the key controls it relies on the provider to perform; review the report, which should contain a description of the key controls tested; and confirm that the design of the control is sufficient to meet management's control objectives.

b) The company typically will need controls that work with those at the service provider. For example, the company should have controls to ensure all transactions are transmitted to the provider for processing. Management should ensure these controls work effectively in combination with the provider's. Most SAS 70 reports include a description of the controls the provider expects its customers to have. This is a section management should review carefully.

c) Management should review the report with care to ensure the testing is sufficient to ensure the adequacy of the controls it will rely on, and then assess the results reported.

If the SAS 70 report identifies deficiencies, management needs to determine what impact the deficiencies have on the controls it relies on at the provider. For example, the report may identify deficiencies in Windows NT servers at an outsourced data center, while the company's software

runs only on UNIX servers. Management may also find that controls within the company compensate or, at least, mitigate the deficiencies.

Service providers do not always provide assurance that any deficiencies will be corrected and retested before the end of their customer's fiscal year. While we believe management should work with the provider to include a commitment to address deficiencies in the contract, the provider may not be responsive. Therefore, management should ensure excellent communications are in place to provide as much notice as possible of potential audit issues.

Outside the United States, providers often do not provide a SAS 70 type II report. Management needs to identify this early and plan accordingly. One option is to pay the provider to obtain such an audit, and another is to develop controls within the company that will address any risks to the financial statements. Finally, management may decide to switch providers to one that provides a SAS 70 type II report.

Additional information on a SAS 70 type II report can be obtained from the external auditor.

8) Fraud Risk Assessment

The concept of a fraud risk assessment is one that has been frequently misunderstood, even though PCAOB AS 2 clearly stated:

> "The auditor should evaluate all controls specifically intended to address the risks of fraud that have at least a reasonably possible likelihood of having a material effect on the company's financial statements."[xxx] [xxxi]

AS 5 contains similar language:

> "…the auditor should evaluate whether the company's controls sufficiently address identified risks of material misstatement due to fraud."

The key to an efficient consideration of fraud is to focus on fraud schemes that could result in a material misstatement of the financials. Many thefts and frauds, while significant and important to prevent or at least detect promptly, are unlikely to result in a material error in the financial statements. (Note: Fraud is assumed in this discussion to include the misappropriation of assets.)

For example:

- The theft of inventory at a company that conducts a full physical inventory at year-end would not result in an error in the year-end financials because a write-off will have been taken.
- The approval and payment of duplicate or excessive payments for services are recorded correctly in the financial statements: the financials correctly reflect the amounts paid, on the appropriate line of the P&L.

There are a number of detailed guides, including guides from each of the major accounting firms, on how to address fraud risk. The high-level approach is to:

- Identify the fraud schemes applicable to the company that might result in a material error in the financials if undetected. Particular attention should be given to schemes involving the management override of controls, including the approval and processing of manual journal entries.
- Identify the key controls that would either prevent or timely detect any such fraudulent activity, and confirm the adequacy of their design.
- Ensure that the identified key controls are tested.

One area of focus relates to restricted access (RA) and segregation of duties (SOD). As discussed earlier in section (a), it is possible to spend a significant amount of time assessing and testing these areas, because many frauds are the result of inappropriate access and especially a combination of access capabilities (e.g., the ability to both set up a vendor and approve invoices). In addition, there are significant business reasons (including the loss of assets) for ensuring appropriate RA and SOD are in place. The key to efficient Section 404 testing for RA and SOD is carefully focusing on access abilities where a resulting fraud could mean the financials are materially misstated. If management desires, additional RA and SOD testing for purely business risk management purposes may be added to Section 404 testing since the added cost of additional testing may be minimal. However, these non-Section 404 tests should be clearly identified as such to the external auditor.

9) Process and Control Documentation

The key business processes and, especially, the material transactions and related controls now need to be documented. There are various techniques and documentation styles for completing the documentation. However, management needs to complete documentation that:

- Enables a reasonably knowledgeable individual — this person does not have to be an expert with experience in the area, but should have some knowledge of the company or its business — to understand the process.
- Provides context for the key controls so that a reasonable person would understand their function.
- Details the operation of key controls, such as identifying who is performing the control, when the control is operating and at what frequency, how the control is performed, what evidence exists that the control was performed, and which reports are used in the operation of the control. It is valuable to agree with the external auditor on the quality standards to be established for control documentation.
- Overall, enables a reasonable person to have a basis upon which to assess the design of the controls: Are the controls identified and documented sufficiently to either prevent or detect a material misstatement?

It is critical to establish a change management process to ensure that documentation is kept up-to-date as processes and controls change. The business does not stop just because of Section 404 requirements. A sound change management process for Section 404 will likely have the following attributes:

- The process is well known to all business process owners.
- Changes to business processes, including computer systems, are identified and the documentation is updated promptly.
- Changes to key controls are identified and assessed promptly, to ensure the potential impact on Section 404 assessment and testing is understood.

KEY POINTS

CHANGE MANAGEMENT

- *It is critical to establish a change management process to ensure that documentation is kept up-to-date as processes and controls change. The business does not stop just because of Section 404 requirements.*

Planned changes, especially those planned for late in the fiscal year, are discussed to ensure the impact on the Section 404 assessment is understood. Consideration is given to delaying the change until after year-end.

G. Testing Key Controls

The SEC's guidance includes an excellent discussion of how to obtain and evaluate evidence that the key controls, and therefore the system of internal control, are operating effectively. Their main points, with added commentary, are:

- "The evaluation of the operating effectiveness of a control considers whether the control is operating as designed and whether the person performing the control possesses the necessary authority and competence to perform the control effectively.
- "The evaluation procedures that management uses to gather evidence about the operation of the controls it identifies as adequately addressing the financial reporting risks for financial reporting elements should be tailored to management's assessment of the risk characteristics of both the individual financial reporting elements and the related controls."

  Comment: two separate assessments of risk are recommended:

  - The risk of a material misstatement arising from the transactions and accounts affected by the control being tested. For example, the higher the balances, the more complex the accounting, the higher the fraud risk, and the greater the judgment being exercised, the greater the risk.
  - The risk that the controls may not operate as designed. Factors affecting this risk might include the complexity of the control, the experience level of the individuals performing it, the level of judgment involved, whether the control has failed in prior period testing, the risk of management override, and the nature of the control (e.g., manual or automated).

The combined effect of these two risks is considered *ICFR risk*.

- "Management should ordinarily focus its evaluation of the operation of controls on areas posing the highest ICFR risk. Management's assessment of ICFR risk also considers the impact of entity-level controls, such as the relative strengths and weaknesses of the control environment, which may influence management's judgments about the risks of failure for particular controls."
- "Evidence about the effective operation of controls may be obtained from direct testing of controls and on-going monitoring activities. The nature, timing, and extent of evaluation procedures necessary for management to obtain sufficient evidence of the effective operation of a control depend on the assessed ICFR risk."

  Comment: monitoring activities relate to activities in the monitoring layer of the COSO internal control framework, as discussed earlier. They may include controls to monitor results of operations and controls to monitor other controls, including activities of the internal audit

function, the audit committee, and self-assessment programs. Where they provide sufficient evidence of the operation of key controls, they represent direct entity-level controls and in the top-down approach discussed above would probably be included as key controls to test.

- "In determining whether the evidence obtained is sufficient to provide a reasonable basis for its evaluation of the operation of ICFR, management should consider not only the quantity of evidence (for example, sample size), but also the qualitative characteristics of the evidence. The qualitative characteristics of the evidence include the nature of the evaluation procedures performed, the period of time to which the evidence relates, the objectivity of those evaluating the controls, and, in the case of on-going monitoring activities, the extent of validation through direct testing of underlying controls."
- "For any individual control, different combinations of the nature, timing, and extent of evaluation procedures may provide sufficient evidence. The sufficiency of evidence is not necessarily determined by any of these attributes individually."
- "In smaller companies, management's daily interaction with its controls may provide it with sufficient knowledge about their operation to evaluate the operation of ICFR. Knowledge from daily interaction includes information obtained by on-going direct involvement with and direct supervision of the execution of the control by those responsible for the assessment of the effectiveness of ICFR.

  "Management should consider its particular facts and circumstances when determining whether its daily interaction with controls provides sufficient evidence to evaluate the operating effectiveness of ICFR. For example, daily interaction may be sufficient when the operation of controls is centralized and the number of personnel involved is limited. Conversely, daily interaction in companies with multiple management reporting layers or operating segments would generally not provide sufficient evidence because those responsible for assessing the effectiveness of ICFR would not ordinarily be sufficiently knowledgeable about the operation of the controls. In these situations, management would ordinarily utilize direct testing or on-going monitoring-type evaluation procedures to obtain reasonable support for the assessment.

KEY POINTS

TESTING KEY CONTROLS

- *Management should always consider the total cost of its Section 404 program, which includes the external auditor's fees. Management can minimize its total costs by maximizing the degree to which the external auditor can reduce their hours through reliance on management testing.*

In theory, management has great flexibility in selecting techniques for testing key controls. It does not have to employ the same techniques (or even the same sampling criteria) as the external auditor. However:

- The testing techniques should clearly provide a reasonable individual sufficient assurance that the controls are operating effectively as documented.
- If self-assessment techniques are used (these are not described here, but information can be obtained on this valuable approach from the internal or external auditor), there has to be a reasonable level of independent confirmation of the self-assessment.
- Testing needs to provide assurance that the controls are operating effectively at year-end, as that is the point in time when the formal assessment is made. For tests performed earlier in the year, steps should be taken to update and roll-forward the results of the tests. Techniques that can be used include a limited reperformance of the earlier tests using fourth quarter transactions, or obtaining re-certifications by process owners of their key controls.
- Testing needs to be performed by competent and trained individuals. A number of organizations are requiring operating management and staff to perform regular testing of their controls. While that may appear to be cost-effective (e.g., it may free internal audit specialists to focus on valuable operational, compliance, and other controls audits), management may need to provide objective reviews and retesting to ensure the tests are performed in accordance with quality standards and the results are reflective of actual operations. This additional review and testing might be performed by internal audit staff or a separate controls testing group. Management should consider the total costs of testing and the most efficient use of resources when staffing the testing program.

This document will not explore in depth the testing techniques that are available. Management should select the approach most suitable for the organization after consultation with experts, including the internal auditor. Some of the techniques available include:

- Traditional testing of controls, such as:
  - Performance of walkthroughs, which confirm the adequacy of the documentation as well as the design of the controls to meet the control objectives.
  - Inquiry, examination, and inspection of related documents to confirm that the control appears to be performed consistently as documented.
  - Reperformance of a sample of transactions to confirm that the control is being performed effectively.
- Continuous auditing, which includes the testing of transactions throughout the period. This is generally assisted with software that selects the transactions to be reviewed.
- Continuous monitoring. This technique generally relies on software to monitor transactions and not only identify transactions for testing, but especially to test 100 percent of the processed transactions for compliance with selected parameters. An example would be a test that identifies purchase orders issued in excess of approved requisitions. The software would report exceptions for assessment as they occur. This technique merits attention and consideration as it may reduce the cost of annual testing, after an initial investment in development.

- Management self-assessment. There are several varieties of this technique, including *management's daily interaction with its controls* as discussed in the SEC guidance. Management needs to consult with testing experts to ensure that the results of any self-assessment provide reasonable, objective evidence that the controls are operating as assessed. The risk is that the individuals performing the assessment may not have direct knowledge of the operation of the control or may not perform a rigorous assessment that verifies the consistency of the control's execution.

Performance of an annual walkthrough of key processes and controls is highly recommended. The external auditor is required to do walkthroughs, which help confirm the accuracy of the documentation and the adequacy of the design of the controls. Walkthroughs by management can, in some cases, be relied on by the external auditor and reduce total costs.[xxxii] Walkthroughs by management are recommended, especially when there have been process or staff changes, as they will detect errors early and ensure management:

- Has a clear and current understanding of the processes and their operation.
- Can identify and correct potential issues early.
- Will perform more efficient testing, as documentation issues have been removed.
- Makes more efficient use of the external auditor's time by ensuring the currency, completeness, and accuracy of the documentation.

Earlier it was stated that management "has great flexibility in selecting techniques to use for testing its key controls." The "in theory" reservation was included because management should always consider the total cost of its Section 404 program. That total cost includes the external auditor's fees. Management can minimize its total costs by maximizing the degree to which the external auditor can reduce their hours through reliance on management testing.

It is still unclear to what extent the external auditor is able to reduce their hours through reliance on management testing when that testing is other than traditional. This is a developing area and merits continued monitoring. However, for the areas where the external auditor is required to perform independent testing and cannot rely on management testing (e.g., control areas assessed as high risk), management may be able to employ less traditional, more cost-effective methods.

1) Testing Automated Controls

In most cases, individuals with IT audit expertise will perform automated control testing; however, management may request IT staff to perform the tests. This is acceptable, but may not allow the external auditor to rely on management testing to reduce the scope of their work.

Where there are good change management controls within ITGC over an application, management may decide to test only a sample of automated controls each year. The principle, called "benchmarking," is described in the PCAOB document issued on May 16, 2005.[xxxiii] The principle needs to be applied to each automated control in turn, examining whether: (a) the software has been changed since the last time it was tested, (b) whether there are sound change management

processes and controls relative to the software, and (c) whether the control is of such significance that risk demands it be tested every year.

In principle, when a company has invested in effective and consistent change management controls, they should have increased assurance that the software — including automated controls — will provide the required functionality on a consistent basis. Management should consider this when planning which automated controls to test. Even if no changes have been made, it is advisable to test at least a sample.

Each of the automated controls, including key reports, need to be tested unless benchmarking applies (see section (d), bullet 8 above); an individual with IT audit experience will usually be able to identify the most appropriate test. Testing will normally consist of one or more of the following:

- Use of test data to confirm the proper operation of the control. The auditor, or IT staff with auditor review and approval, will enter transactions in the test environment and confirm the control operates as documented.
- Examination of related application code, a common technique when SAP is the application and where SAP configuration tables can be reviewed. The auditor must possess a solid understanding of the software configurations or code to perform this test.
- Use of separate audit software to re-perform the functionality. For example, the auditor may use ACL or a Business Objects report to select and age open accounts receivable transactions and compare the results to the reports used by management.
- Manual re-performance of the control. In a few cases, where the control is not complex and the data not voluminous, the auditor may be able to recalculate totals or otherwise re-perform the specific functionality of the key control.

Unless there are concerns in ITGC that indicate otherwise, automated controls need only be tested once each year (subject to benchmarking, as discussed previously). If ITGC issues indicate there is a significant risk that unauthorized, unapproved, or untested changes may be made to the automated controls, the frequency of testing should be increased with special attention given to year-end closing processes.

2) Testing Indirect Entity-level Controls

When it comes to obtaining assurance of the design and operation of indirect entity-level controls, such as the ethical values of the organization and the effectiveness of audit committee oversight, management again has more options than the external auditor. This is because, as recognized by the SEC and previously in AS 2, management has more direct exposure to and knowledge of its operations.

Management should review each key control in this area and determine the more appropriate method to obtain assurance:

- Traditional sampling and testing (e.g., reviewing audit committee minutes to confirm the members reviewed the interim and annual financial statements).
- Management self-assessment (e.g., obtaining confirmations from direct management that the ethics policy is made available to all new employees).
- Surveys (e.g., surveying all or a substantial portion of the employees and obtaining their confidential assessment of the ethical environment, conformance to company policy, etc.).

The external auditor may be able to rely on or join management in performing tests of indirect entity-level controls. Management should, therefore, explore this possibility with the external auditor during annual planning.

H. Assessing the Adequacy of Controls, Including Assessing Deficiencies

If all key controls are properly identified, assessed as adequately designed, and the results of testing indicates they are all operating effectively, management will be able to assess its overall system of ICFR as effective. But, in real life, exceptions are identified in testing. A number of key controls could be deemed to be missing, deficient in design, or not operating effectively.

Management needs to decide whether these deficiencies mean that the system of internal control does not provide a reasonable level of assurance that there will not be material errors in future financial statements.

This is achieved by assessing each control deficiency in turn to determine the likelihood of an error in the financial statements and its potential magnitude. Each deficiency is assessed to determine whether it is *material*, *significant*, or neither. Then, management needs to determine whether a combination of deficiencies[1] is likely to represent a risk (i.e., an *aggregated* risk) that is material or significant.

Although the scope of both management's and the external auditor's assessment of internal control is focused on the risk of a material misstatement of the financial, any deficiencies have to be assessed first to determine whether they are material weaknesses, and then whether they are significant deficiencies. Only material weaknesses affect management's assessment and have to be disclosed in the annual financial statements; however, significant deficiencies must be identified and reviewed with the audit or equivalent committee.

The following definitions use the terms *material error,* as discussed above, and *reasonable possibility*. The latter is related to the term *reasonable assurance*, means that there is at least a reasonable likelihood, and is generally understood to be in the 5 percent to 10 percent probability range.

KEY POINTS

ASSESSING THE ADEQUACY OF CONTROLS

- *If all the key controls are properly identified, assessed as adequately designed, and the results of testing indicates they are all operating effectively, management is able to assess its overall system of internal control over financial reporting as effective.*
- *This evaluation requires an exercise of judgment, based on an assessment of what constitutes reasonable assurance under the circumstances, not on the mechanical application of a predetermined probability formula.*

1 As noted earlier, the key to an aggregated risk is that the controls are likely to fail at the same time because, for instance, they are performed at the same time by the same people, or using the same computer system.

A *material weakness* is one where there is a *reasonable possibility* that an error that is *material* to the financial statements would neither be prevented nor detected within a reasonable period of time. It is defined the same way in the SEC and PCAOB guidance:

> "…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."

A *significant* deficiency is less severe. It was redefined in AS 5 and the SEC guidance for management:

> "…a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness yet important enough to merit attention by those responsible for oversight of the company's financial reporting."

External audit firms have historically adopted a framework for assessing deficiencies.[xxxiv] This approach is important for management to consider because it may be followed by the external auditor, although it is not referenced in AS 5. However, there is no requirement for management to follow precisely the same process.

Management should adopt a principles-based approach, relying on their judgment, rather than a strict rules-based approach. The PCAOB similarly advised external auditors in a November 2005 report to rely on their professional judgment when assessing deficiencies:

> "This evaluation requires an exercise of judgment, based on an assessment of what constitutes reasonable assurance under the circumstances, not on the mechanical application of a predetermined probability formula. Inspectors observed, however, that the quest for quantitative rules of thumb in the application of the definitions described above may have resulted in some auditors exercising less judgment than the standard requires in this area. Many engagement teams used a framework developed through the collective effort of nine firms for evaluating deficiencies. That framework uses terms such as 'gross exposure,' 'adjusted exposure,' and 'upper-limit deviation rate.' The statistical precision suggested by these terms may have driven auditors' decision-making process unduly toward simplistic quantitative thresholds and away from the qualitative evaluation that may have been necessary in the circumstances.
>
> "This evaluation framework can result in decisions that are consistent with the provisions of Auditing Standard No. 2. Further, the use of the framework promoted consistency among different audit teams within and across firms. Nevertheless, the framework is not a substitute for the professional judgment that Auditing Standard No. 2 requires. Moreover, using this framework could, in some cases, lead auditors to spend more time evaluating the severity of a deficiency than otherwise would be necessary."

Management's process must ensure the following are considered:

1. **Could there be an error in the financial statements as a result of the control deficiency?** If the answer is no, the process can stop and the deficiency assessed as neither significant nor material. Management should further reassess whether this should remain a key control.

   With respect to deficiencies in ITGCs, management should follow the risk assessment in reverse order. They should identify: what IT control objective is impacted and to what extent; whether the IT control objective should be considered not to have been achieved; what applications and critical IT functionality the IT control objective addresses; what critical IT functionality involved; and, what risk there is of an error in the financials.[1]

   Indirect entity-level controls also require special handling to determine what controls and processes may be impacted. It is not sufficient to simply say these controls are pervasive. Instead, management needs to address specifics relative to risk to the financial statements. For example, if there are problems hiring trained accounting staff, what processes and controls are involved? In addition, are there sufficient management-level reviews and key controls that would detect or prevent errors?

2. **Are there compensating or mitigating controls** (they must be key controls that have tested effective)? To what extent do they reduce the risk? If the answer is that the risk is fully addressed, the process can stop and the deficiency assessed as neither significant nor material. Management should further reassess whether this should remain a key control as it may be redundant.

3. **Could the deficiency result in a material misstatement of the financials?** The assessment must consider where the error would occur in the financial statements. It is relatively straightforward when the error is in the P&L. However, if the effect is only on balance sheet accounts, the error should be considered using a materiality gauge related to that account rather than the traditional P&L measure.

   If the error would affect a disclosure, management needs to consider whether the error is material relative to the disclosed amounts and the significance to the investors, and potentially the regulators, of the specific disclosure. One measure that might be considered is whether the identification of an error of such an amount in a prior period's financial statements would result in needing to restate those financials.

KEY POINTS

MATERIAL DEFICIENCIES

- *Does management truly believe and would a reasonable person concur that the probability of a material error in future financial statements, which would not be detected by other controls, is in the 5 percent to 10 percent range or more?*
- *Would the deficiency prevent a prudent official from concluding that he or she has reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles.*

1 Detailed guidance in the assessment of ITGC deficiencies can be obtained from the internal auditor or The IIA's website at www.theiia.org.

4. **Is the risk of a material misstatement reasonably possible?** The next step is to assess the likelihood of that happening. As previously stated, *reasonably likely* is generally considered to be in the 5 percent to 10 percent range.

5. **Would a reasonable individual assess the deficiency as material?** This is the key *acid test*. Given that management may not assess its system of ICFR as effective once it identifies a material weakness, it should ask additional questions to validate the assessment of a deficiency as material.

   a. Does management truly believe and would a reasonable person concur that the probability of a material error in future financial statements, which would not be detected by other controls, is in the 5 percent to 10 percent range or more? In their November 30, 2005 report, the PCAOB stated:

      "The definitions in the standard … are designed to lead to a determination as to whether the deficiency would prevent a prudent official from concluding that he or she has reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with generally accepted accounting principles.

      "Further, the terms 'probable,' 'reasonably possible,' and 'remote,' should not be understood to provide for specific quantitative thresholds. Proper application of these terms involves a qualitative assessment of probability. Therefore, the evaluation of whether a control deficiency presents a 'more than remote' likelihood of misstatement can be made without quantifying the probability of occurrence as a specific percentage."

   b. If the assessment of a deficiency is based on prior period errors, perhaps resulting in the restatement of prior period financials, is it reasonable to assess the current condition of internal controls (and therefore identify a material weakness) as ineffective?

      This issue (assessing controls following a restatement) has become topical. While some external auditors have taken the position that there must be a material weakness if the financials are being restated, that is neither the position of the SEC nor the PCAOB.

      AS 5 describes the "restatement of previously issued financial statements to reflect the correction of a material misstatement" as an indicator of a material weakness, but has not directed that it must be assessed as such.

      Both the SEC and PCAOB have indicated that while there is at least a significant deficiency, the underlying facts and circumstances must be considered. For example, if controls are improved in the current period by hiring additional technical accountants who then identify prior period accounting errors, then the current condition of internal controls is sound. This is because the material weakness was in the prior and not in the current period. On the other hand, if the error was detected by the external auditor and

should have been, but was not, detected internally, this may indicate a material weakness in the internal staff's technical competence.

6. **If the deficiency is not a material weakness, should it be disclosed to the audit committee as a significant deficiency?** Significant deficiencies need to be reported only to the audit or equivalent committee, and management is not required to disclose them in either the quarterly or annual reports filed with the SEC.

   Management should give strong consideration to sharing any issues with the audit committee that are borderline significant deficiencies because this is prudent. It should also be noted that the remediation of a significant deficiency is probably[xxxv] a material change in the system of internal control and should be reported in the interim period within which it occurs.

Material weaknesses need to be considered and will affect both the quarterly Section 302 certification and the annual Section 404 assessment, if they are not corrected prior to year-end. Because the Section 404 assessment is as of year-end, management has the opportunity to achieve a clean opinion if it can identify the deficiency early, implement corrective actions, and test the corrected operations prior to year-end. The external auditor will also need to test the operation of remediated controls.

I. Management's Report on Internal Controls — the End Product

Whether in the annual assessment for Section 404 or the quarterly certification for Section 302, the language of management's report will be based substantially on the advice of counsel. However, there are certain drivers that management should consider:

1. Management has a great deal of latitude in describing the condition of its internal controls. The only formal requirement is that it not assess the controls as effective when there is a material weakness. Other requirements are being defined over time as the SEC responds to filings and sets expectations for content (counsel can advise on these matters).

2. The assessment should clearly describe management's opinion. What is the true condition of the system of internal control at the end of the year? Is it sufficiently robust to provide reasonable assurance that material errors will be either prevented or detected? The investor should be able to read the assessment and understand whether the company has adequate controls to run the business and report the results. (This is especially true when there is pressure to report a material weakness as a result of accounting errors in a prior period. Management should determine whether the current system of internal control is adequate, providing reasonable comfort related to the reliability of future financial statements, and not report deficiencies they do not believe relate to the current condition or future filings. In these circumstances, management may feel pressure to follow the rules at the expense of the principles. The assessment should reflect management's assessment of the controls and not mislead the investor regarding their effectiveness.)

3. The root cause of deficiencies should be understood. Control failures may be symptoms of a larger problem related to resources or management. The overall system will not be corrected until the larger problem is resolved, and, when known, the root cause should be reported. That is the true deficiency.

KEY POINTS

THE END PRODUCT

- *Management has a great deal of latitude in describing the condition of its internal controls. The only formal requirement is that it not assess the controls as effective when there is a material weakness.*
- *The assessment should clearly describe management's opinion. What is the true condition of the system of internal control at the end of the year? Is it sufficiently robust to provide reasonable assurance that material errors will either be prevented or detected? The investor should be able to read the assessment and understand whether the company has adequate controls to run the business and report the results.*

4. When deficiencies are reported, sufficient related information should be provided to enable the investor to understand their significance, the risk they represent, and how management will ensure the integrity of future financial statements.

J. Closing Thoughts on Efficiency

Most will agree that the Section 404 requirement has improved the quality of internal control systems through increased attention by both management and the external auditor. However, there is less than universal agreement that the improvement has been justified relative to the enormous cost.

The following checklist may help management teams ensure their Section 404 program is efficient.

KEY POINTS

EFFICIENCY

- *Is the Section 404 program assessed for effectiveness on a continuing basis, to ensure it is improved as the organization learns from experience and benefits from changes in regulations or their interpretation?*

1. Has operating management taken ownership of their processes and documentation, rather than leaving it to the Section 404 team or the internal auditing function?
2. Does operating management update all process and control documentation promptly throughout the year and not just when testing starts? Is there an effective change management process in place, including the timely assessment of process changes for their potential impact on key controls?
3. Is operating management committed to assess and remediate all control deficiencies promptly? In situations where remediation is not justified based on management's assessment of risk and cost, is management committed to communicating that decision promptly so the effect on management's overall assessment of controls can be identified and discussed with senior management?
4. Has a top-down, risk-based approach been used to identify the key controls? Is management confident that all identified key controls are truly key? Has the design of the related processes been reviewed to determine if changes can result in fewer and more effective controls, relying more on automated controls or on higher-level controls (e.g., detailed reconciliations and flux analyses)? The fewer the controls to test, the lower the cost.
5. Is management of the Section 404 program at a sufficiently high level within the organization to:
   - Influence operating management relative to completion of their responsibilities?
   - Communicate effectively with executive management the program's progress and potential issues?
   - Negotiate as needed with the external auditor (e.g., to increase reliance on management testing, agree on key controls early, and address concerns as they arise)?

6. Is the use of internal resources optimized, including the use of internal auditors to perform testing or to validate testing performed by management staff?
7. Has overall staffing been optimized, reducing reliance on more expensive external consultants and testers?
8. Has reliance by the external auditor on management testing been optimized?
9. Does the external auditor follow a top-down, risk-based approach as required by AS 5?
10. Is there a detailed project plan:
    a. That includes a walk-through of all significant processes early in the year, preferably in the first quarter?
    b. With testing scheduled in such a way that all key controls are tested by mid-year, with additional testing to update the results scheduled closer to year-end? This enables the external auditor to start their walkthroughs and testing early, providing time for management to address and remediate any deficiencies identified in either management or external auditor testing.
    c. That includes all key activities required to complete the program, such as fraud risk assessment, consideration of any end-user computing issues, assessment of SAS 70 reports from service providers, etc.?
    d. Detailing all required resources, including specialists (e.g., for IT or tax processes and controls), so they can be scheduled early?
    e. With regular reporting to senior management that focuses on key metrics and issues, such as:
        - Progress against timetables, highlighting steps that are or may be behind schedule?
        - Percentage of key controls tested compared to their scheduled completion level?
        - Number and percentage of key controls that are failing?
        - Number of failed controls that are potentially significant to the Section 404 assessment?
        - The number of failed controls where remediation will not be completed within 30 days, so senior management can focus on a timely completion?
        - The number of key controls where remediation and retesting may not be completed with sufficient time for the external auditor to retest (these are likely to be open deficiencies at year-end)?
        - Costs to date and projected through the end of the year?
        - Potential resource issues?
        - Other issues, such as coordination and concerns raised by the external auditor?

11. Has there been communication and coordination with all service providers to ensure that a SAS 70 type II report will be available at the appropriate time, and that early warning is provided of potential deficiencies being identified during the SAS 70 audit?

12. Finally, is the Section 404 program itself assessed for effectiveness on a continuing basis, to ensure it is improved as the organization learns from experience and benefits from changes in regulations or their interpretation?

Acknowledgments

The IIA would like to thank Norman Marks as the author of both editions of this guide and the members of The IIA's International Professional Issues Committee, partners with external audit firms, representatives of regulatory agencies, and internal audit thought leaders who took the time to review drafts and provide constructive suggestions for improvement:

- Abraham Akresh.
- David Bentley.
- Raquel Filipek.
- Sam Fogleman.
- Kiko Harvey.
- Roger Herd.
- Heriot Prentice.
- Harold Silverman.
- Curt Verschoor.

Notes

[i] Included in the quarterly financial statements filed on Form 10-Q with the SEC.

[ii] Of note is this excerpt from Institutional Shareholder Services, *ISS U.S. Corporate Governance Policy — 2006 Updates*:

> "Companies with significant material weaknesses identified in the Section 404 disclosures potentially have ineffective internal financial reporting controls, which may lead to inaccurate financial statements, hampering shareholders' ability to make informed investment decisions, and may lead to the destruction in public confidence and shareholder value."

[iii] Executives at some companies have informed the authors that their external auditors told them that if they have more than a specified number of control deficiencies, they may not assess their controls as effective. Others have been told that specific deficiencies (e.g., failing to monitor the activities of the database administrator, or failing to have a comprehensive fraud assessment program) are always at least significant and probably material deficiencies. These specific cases are not consistent with the language — and we believe the intent — of AS 5 or the guidance from the SEC. While some may disagree, AS 5 is fundamentally a principles-based standard that emphasizes the use of judgment by both management and the external auditor.

[iv] In the Introduction to AS 5, the PCAOB states:

> "…the Board has been 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 and information 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.
>
> "The auditor is required to provide an independent opinion on the effectiveness of the company's internal control over financial reporting. The auditor does not have the familiarity with the company's controls that management has and does not interact with or observe 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 observation of or 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 on-going basis."

[iv] In this Guide, the terms *material error* and *material misstatement* have been used interchangeably to represent the risk of a material error in the financial statements filed with the SEC, regardless of whether the error is the result of fraud or an inadvertent control failure.

[vi] In AS 5, the PCAOB used the term *reasonably possible*. In developing the rules for the Section 404 report, the SEC used the term *reasonably likely*, which is also used in the Section 302 certification. In this guide, we have used the terms synonymously to mean more than remote but less than probable.

[vii] In the Introduction to the Standard, paragraph 3.

[viii] *Report On The Second-Year Implementation Of Auditing Standard No. 2, An Audit Of Internal Control Over Financial Reporting Performed In Conjunction With An Audit Of Financial Statements*, PCAOB Release No. 2007–004, April 18, 2007.

[ix] The user of the Section 404 assessment should understand that the quality of the system of internal control as of the reporting date is only an *indication* of future results and depends, among other matters, on there being no significant change to the ICFR. It should be noted that the PCAOB requires (in AS 5) that the report of the external auditors include the following statement: "Projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate."

[x] The role of the internal auditing function in Section 404 testing has been discussed in detail in The IIA's *Internal Auditing's Role in Sections 302 and 404 of the Sarbanes-Oxley Act*, which was released on May 26, 2004. Key points addressed in the document related to assistance with testing include:

> "It is management's responsibility to ensure the organization is in compliance with the requirements of Sections 302 and 404 and other requirements of the Act, and this responsibility cannot be delegated or abdicated. Support for management in the discharge of these responsibilities is a legitimate role for internal auditors. The internal auditors' role in their organization's Sarbanes-Oxley project can be significant, but also must be compatible with the overall mission and charter of the internal audit function. Regardless of the level and type of involvement selected, it should not impair the objectivity and capabilities of the internal audit function for covering the major risk areas of their organization. Internal auditors are frequently pressured to be extensively involved in the full compendium of Sarbanes-Oxley project efforts as the work is within the natural domain of expertise of internal auditing." (Executive Summary)
>
> "Activities that are included in the internal auditor's recommended role in supporting the organization in meeting the requirements of Sections 302 and 404 include:
>
> - Project Oversight.
> - Consulting and Project Support.
> - Ongoing Monitoring and Testing.
> - Project Audit."
>
> (Recommended Role of Internal Audit)
>
> "Ongoing Monitoring and Testing
>
> - Advise management regarding the design, scope, and frequency of tests to be performed.
> - Independent assessor of management testing and assessment processes.
> - Perform tests of management's basis for assertions.
> - Perform effectiveness testing (for highest reliance by external auditors).
> - Aid in identifying control gaps and review management plans for correcting control gaps.
> - Perform follow-up reviews to ascertain whether control gaps have been adequately addressed.
> - Act as coordinator between management and the external auditor as to discussions of scope and testing plans.
> - Participate in disclosure committee to ensure that results of ongoing internal audit activities and other examination activities, such as external regulatory examinations, are brought to the committee for disclosure consideration."
>
> (Recommended Role of Internal Audit)

[xi] The SEC provided guidance, in its January 2002 FAQ number 22, that a formal evaluation of internal controls (similar to that required for Section 404) is not required by current regulations to complete the section 302 certification. Their answer to FAQ 22 is excerpted in note [xxxv] below.

[xii] Small businesses and foreign filers will use the equivalent forms, 10-K SB and 20-F.

[xiii] It is notable that the U.S. Foreign Corrupt Practices Act of 1977 directed that internal controls are the responsibility of management.

[xiv] AS 5's definition is based on that in COSO, as is that in Codification of Statements on Auditing Standards Section 319 (Auditing Standards Section 319).

[xv] Securities Exchange Act Rules 13a-15(f) and 15d-15(f).

[xvi] COBIT 4.0 is available at www.isaca.org/cobit.

[xvii] This is described further in *A Framework for Internal Auditing's Entitywide Opinion on Internal Contro*l (The IIA Research Foundation, 2004) and *Internal Audit Reporting Relationships: Serving Two Masters* (The IIA Research Foundation, 2003).

[xviii] First mentioned in an SEC release in August 2002, and incorporated into the U.S. Securities Exchange Act of 1934 (as amended) Rules 13a-15(e) and 15d-15(e).

[xix] In their October 2004 *Frequently Asked Questions* report, the SEC addressed in question 23 whether the assessment of ICFR included required supplementary schedules. As indicated below, their conclusion was that the assessment does not currently need to be included within the scope of that assessment.

> "Q: The Commission's rules implementing Section 404, announced in Release No. 34-47986, require management to perform an assessment of internal control over financial reporting which includes the "preparation of financial statements for external purposes in accordance with generally accepted accounting principles." Does management's assessment under the Commission's rule specifically require management to assess internal control over financial reporting of required supplementary information? Supplementary information includes the financial statement schedules required by Regulation S-X as well as any supplementary disclosures required by the FASB. One of the most common examples of such supplementary information is certain disclosures required by the FASB Standard No. 69, Disclosures about Oil and Gas Producing Activities.
>
> "A: Adequate internal controls over the preparation of supplementary information are required and therefore should be in place and assessed regularly by management. The Commission's rules in Release No. 34-47986 did not specifically address whether the supplementary information should be included in management's assessment of internal control over financial reporting under Section 404. A question has been raised as to whether the supplementary information included in the financial statements should be encompassed in the scope of management's report on their assessment of internal control over financial reporting.
>
> "The Commission staff is considering this question for possible rule making. Additionally, the Commission staff is evaluating broader issues relating to oil and gas disclosures and will include in its evaluation whether rulemaking in this area may be appropriate. Should there be any proposed changes to the current requirements in this area, they will be subject to the Commission's standard rule-making procedures, including a public notice and comment period in advance of rule making. As a result, internal control over the preparation of this supplementary information need not be encompassed in management's assessment of internal control over financial reporting until such time that the Commission has completed its evaluation of this area and issues new rules addressing such requirements."

[xx] Current reports include Form 6-K, definitive proxy materials, and definitive information statements.

[xxi] In their final rules implementing Section 404, the SEC made the following comments related to the difference between internal controls over financial reporting and disclosure controls. Please note the highlighted section:

> "We agree that some components of internal control over financial reporting will be included in disclosure controls and procedures for all companies. *In particular, disclosure controls and procedures will include those components of internal control over financial reporting that provide reasonable assurances that transactions*

are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles. However, in designing their disclosure controls and procedures, companies can be expected to make judgments regarding the processes on which they will rely to meet applicable requirements. In doing so, *some companies might design their disclosure controls and procedures so that certain components of internal control over financial reporting pertaining to the accurate recording of transactions and disposition of assets or to the safeguarding of assets are not included.* For example, a company might have developed internal control over financial reporting that includes as a component of safeguarding of assets dual signature requirements or limitations on signature authority on checks. That company could nonetheless determine that this component is not part of disclosure controls and procedures. *We therefore believe that while there is substantial overlap between internal control over financial reporting and disclosure controls and procedures, many companies will design their disclosure controls and procedures so that they do not include all components of internal control over financial reporting*."

We concur with the SEC's observation that the referenced controls could be part of a company's system of internal control and, yet, not be included in disclosure controls. However:

- As noted by the SEC, disclosure controls will include all the components of internal control over financial reporting required to provide reasonable assurance over the reliability of the financial statements. By definition, those are key controls.
- The controls that the SEC has referenced as examples of controls that are included in ICFR, but excluded from disclosure controls, would *not* be considered key controls for Section 404 purposes.

Therefore, while the SEC's position is that there is only "substantial overlap" between ICFR and disclosure controls, in practice we believe there will be few situations where key controls for Section 404 are not included in disclosure controls.

Some experts, including certain specialized attorneys, have taken a different approach. Arguments include:

- Disclosure controls only relate to the design of controls and not to their operation. If a material weakness relates only to the operation of a control (i.e., it is adequately designed, but not consistently followed), these experts believe management can report an ineffective system of internal control for Section 404, but an effective system of disclosure controls for Section 302. However, we believe such a determination is likely to confuse rather than inform investors.
- Safeguarding of assets is included in the scope of internal controls for Section 404, but not in disclosure controls for Section 302. However, ICFR for Section 404 relates to controls that prevent or detect a misstatement of the financials. A misstatement of the financials filed with the SEC is, by definition, within the scope of disclosure controls.

[xxii] In this guide, the term *interim assessment* of internal controls or disclosure controls is used to refer to what the SEC describes as the *periodic evaluation* of those controls.

[xxiii] Some companies and external auditors have considered materiality relative to interim financial statements when defining significant accounts. In their May 2005 Staff Report, the SEC made it clear that:

> "Companies generally should determine the accounts included within their Section 404 assessment by focusing on annual and company measures rather than interim or segment measures. If management identifies a deficiency when it tests a control, however, at that point it must measure the significance of the deficiency by using both quarterly and annual measures, also considering segment measures where applicable."

[xxiv] In the first few years of Section 404 assessments, on the advice of the external auditor, many companies adopted a lower measure called *planning materiality*. They would establish materiality at 5 percent of pre-tax income and then a lower level — perhaps half that number — as planning materiality. In some cases, they took a further "haircut" based on perceived risk levels — perhaps another 10 percent — to establish planning materiality. All accounts above planning materiality would then be determined to be significant accounts.

This is no longer seen as appropriate, as it brings into scope accounts where there is less than a reasonable possibility of a material error.

Other companies have decided that using a reduced materiality level, similar to planning materiality, is advisable because it is prudent. While ensuring that there are adequate controls to prevent or detect errors that are less than material is a sound objective, there is no need to include these accounts in scope and subject to external auditor testing. Our advice is to include in scope only significant accounts as described in this guide. Key controls over the smaller accounts may be described as *key business controls*, subject to periodic testing by management or the internal auditor.

[xxv] Appendix B, under Multiple Locations Scoping Decisions.

[xxvi] The PCAOB has removed the requirement from AS 5, previously in AS 2, to understand key business processes and transactions. This is to allow flexibility in approach by the external auditor. We include it in the guide because we have found this approach valuable in practice.

[xxvii] The IIA's *Guide to the Assessment of IT General Controls Scope based on Risk* was first published in January 2007. In its first six months, GAIT was downloaded nearly 10,000 times and its use is becoming widespread, not only within the United States, but also in Europe and Asia. GAIT was updated to reflect changes in PCAOB and SEC guidance in August 2007 and can be found on The IIA's Web site at www.theiia.org.

[xxviii] In its guidance for management, the SEC uses the term *critical functionality* to refer to all functionality relied upon that is not an automated control (text in footnotes in the SEC document have been replaced by text in parentheses):

> "Controls that management identifies as addressing financial reporting risks may be automated (for example, application controls that perform automated matching, error checking, or edit checking functions), dependent upon IT functionality (for example, consistent application of a formula or performance of a calculation and posting correct balances to appropriate accounts or ledgers), or a combination of both manual and automated procedures (for example, a control that manually investigates items contained in a computer generated exception report). In these situations, management's evaluation process generally considers the design and operation of the automated or IT-dependent application controls and the relevant IT general controls over the applications providing the IT functionality. While IT general controls alone ordinarily do not adequately address financial reporting risks, the proper and consistent operation of automated controls or IT functionality often depends upon effective IT general controls. The identification of risks and controls within IT should not be a separate evaluation. Instead, it should be an integral part of management's top-down, risk-based approach to identifying risks and controls and in determining evidential matter necessary to support the assessment.
>
> "Aspects of IT general controls that may be relevant to the evaluation of ICFR will vary depending upon a company's facts and circumstances. For purposes of the evaluation of ICFR, management only needs to evaluate those IT general controls that are necessary for the proper and consistent operation of other controls designed to adequately address financial reporting risks. For example, management might consider whether certain aspects of IT general control areas, such as program development, program changes, computer operations, and access to programs and data, apply to its facts and circumstances. Specifically, it is unnecessary to evaluate IT general controls that primarily pertain to efficiency or effectiveness of a company's operations, but which are not relevant to addressing financial reporting risks."

[xxix] Management can reference the PCAOB's answer to question 24 on service organizations in its *Staff Questions and Answers,* issued on June 23, 2004.

[xxx] Paragraph 24 of AS 2.

[xxxi] SAS 99 makes a similar statement: "For purposes of the Statement, fraud is an intentional act that results in a material misstatement in financial statements that are the subject of an audit."

[xxii] Some companies have gained efficiencies by conducting joint walkthroughs with the external auditors; this is more likely when the management testing is performed by the internal auditing function.

[xxxiii] The PCAOB discussed benchmarking in its *Staff Questions and Answers*, issued on May 16, 2005, No. 45:

> "In general, to render an opinion as of the date of management's assessment, the auditor needs to test controls every year. This type of evidence is needed regardless of whether controls were found to be effective at the time of the prior annual assessments or whether those controls have changed since that time, because even if nothing significant changed about the company — the business model, employees, organizational structure, etc. — controls that were effective last year may not be effective this year due to error, complacency, distraction, and other human conditions that result in the inherent limitations in internal control over financial reporting. . Automated application controls, however, will continue to perform a given control (for example, aging of accounts receivable, extending prices on invoices, performing edit checks) in exactly the same manner until the program is changed. Entirely automated application controls, therefore, are generally not subject to breakdowns due to human failure and this feature allows the auditor to 'benchmark' or 'baseline' these controls.
>
> "If general controls over program changes, access to programs, and computer operations are effective and continue to be tested, and if the auditor verifies that the automated application control has not changed since the auditor last tested the application control, the auditor may conclude that the automated application control continues to be effective without repeating the prior year's specific tests of the operation of the automated application control. The nature and extent of the evidence that the auditor should obtain to verify that the control has not changed may vary depending on the circumstances, including depending on the strength of the company's program change controls.
>
> "When using a benchmarking strategy for a particular control, the auditor also should consider the importance of the effect of related files, tables, data, and parameters on the consistent and effective functioning of the automated application control. For example, an automated application for calculating interest income might be dependent on the continued integrity of a rate table used by the automated calculation.
>
> "To determine whether to use a benchmarking strategy, the auditor should evaluate the following factors. As these factors increase in significance, the control being evaluated should be viewed as well suited for benchmarking. As these factors decrease in significance, the control being evaluated should be viewed as less suited for benchmarking. These factors are:
>
> - the extent to which the application control can be matched to a defined program within an application;
> - the extent to which the application is stable (i.e., there are few changes from period to period); and whether a report of the compilation dates of all programs placed in production is available and is reliable. (This information may be used as evidence that controls within the program have not changed.)
>
> "Benchmarking automated application controls can be especially effective for companies using purchased software when the possibility of program changes is remote — for example, when the vendor does not allow access or modification to the source code.
>
> "At some point, the benchmark of an automated application control should be reestablished. To determine whether to reestablish a benchmark, the auditor should evaluate the following factors:
>
> - the effectiveness of the IT control environment, including controls over application and system software acquisition and maintenance, access controls and computer operations;
> - the auditor's understanding of the effects of changes, if any, on the specific programs that contain the controls;
> - the nature and timing of other related tests; and
> - the consequences of errors."

[xxxiv] The framework was developed by nine CPA firms in association with a respected academic. It can be found on the Financial Executives International's Web site at www.financialexecutives.org/.

[xxxv] We recommend consulting with SEC counsel, although it appears reasonable to assume that if a material weakness is material to the investor, then its resolution is highly likely to be a material change in the system of internal controls — and similarly likely to be material to the investor.

> In January 2002, SEC staff issued answers to a number of Frequently Asked Questions. The answer to question 22 is relevant, and key portions are highlighted in the extract below:
>
> "Although proposed amendments to Exchange Act Rules 13a-15 and 15d-15 would impose a requirement on an issuer's management to conduct an evaluation, with the participation of the issuer's CEO and CFO, of the effectiveness of the issuer's internal controls and procedures for financial reporting …, the Commission's rules currently do not specifically require an issuer's CEO or CFO, or the issuer itself, to conduct periodic evaluations of the issuer's internal controls or the issuer's internal controls and procedures for financial reporting. Some elements of internal controls are included in the definition of disclosure controls and procedures. There is a current evaluation requirement involving the CEO and the CFO of that portion of internal controls that is included within disclosure controls and procedures as part of the required evaluation of disclosure controls and procedures. We expect that issuers generally also would engage in an evaluation of internal controls. We believe that issuers generally currently evaluate internal controls, for example, in connection with reviewing compliance with Section 13(b) of the Exchange Act or in connection with the preparation or audit of financial statements.
>
> " … to the extent that an issuer has conducted an evaluation of its internal controls as of the end of the period covered by the report, including under the circumstances described in the preceding paragraph, ***the issuer should disclose any significant changes to the internal controls*** or in other factors that could significantly affect these controls subsequent to the date of their evaluation, ***including any corrective actions with regard to significant deficiencies and material weaknesses***. If the issuer has made any significant changes to internal controls or in other factors that could significantly affect these controls, such changes would presumably follow some evaluation, in which case the required disclosure must be made."

The Institute of Internal Auditors

PROFESSIONAL GUIDANCE

Setting the Standard