Sarbanes-Oxley Act: Section 404 Practical Guidance for Management*

July 2004

*connectedthinking

PricewaterhouseCoopers

This monograph is designed to assist management in its efforts to satisfy its responsibilities established by the Public Company Accounting Reform and Investor Protection Act of 2002. The monograph is based on rule-making and guidance available as of July 2, 2004; accordingly, as new rules or modifications or interpretations to existing rules emerge, certain aspects of this monograph may become obsolete. Because interpreting this guidance is proving to be an evolutionary process, preparers and users are cautioned to carefully evaluate and monitor further implementation guidance from the Securities and Exchange Commission (SEC) and the Public Company Accounting Oversight Board (PCAOB). PricewaterhouseCoopers will continue to monitor regulatory activities, company interpretations, and evolving practices; we will update our policies and will issue updated perspectives as warranted. In providing the information contained in this monograph, PricewaterhouseCoopers is not engaged in rendering legal, or other professional advice and services. As such, this monograph should not be used as a substitute for consultation with professional, legal, or other competent advisors.

PRICEWATERHOUSECOOPERS

To Our Clients and Friends:

The Public Company Accounting Reform and Investor Protection Act of 2002 (the Act or the Sarbanes-Oxley Act) requires public companies to develop new practices involving corporate governance and financial reporting with the objective of restoring the public trust in the capital markets. One of the most challenging aspects of the Act's requirements involves a company's responsibilities for internal controls.

Entitled *Management Assessment of Internal Controls,* Section 404 of the Act (Section 404) stipulates that public companies must take responsibility for maintaining an effective system of internal control, in addition to reporting on the system's effectiveness. The Act requires most public companies (i.e., accelerated filers that meet certain market capitalization requirements) to report annually on the company's internal control over financial reporting for fiscal years ended on or after November 15, 2004. The majority of the remaining public companies, including foreign private issuers, will be required to comply with these requirements for fiscal years ended on or after July 15, 2005.

While Section 404 poses numerous challenges for preparers, users, and external auditors – both in implementing the mandate and understanding its implications – this monograph is primarily designed to address the challenges facing preparers.

We fully recognize that implementation, particularly in the critical first year, will present preparers with many challenges, complexities, and new costs. However, for the benefits of Section 404 to be realized by all of the participants in the capital markets, a substantial effort will be needed. A thorough assessment and evaluation of internal control over financial reporting will go a long way to achieving a fundamental objective of Section 404: restoring investor confidence in financial reporting. This monograph is presented to you in that spirit.

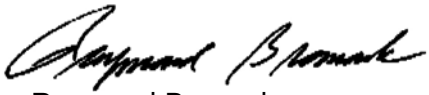
The monograph is one in a series of publications[1] that we have issued in relation to the Sarbanes-Oxley Act. This monograph describes the key activities integral to a successful Section 404 assessment process including, among others, scoping, documenting, testing, evaluating, and reporting. It reflects the insights and perspectives we have gained by working with our clients and obtaining input from the many PricewaterhouseCoopers' partners and staff who have concentrated significant amounts of time on understanding this new reporting model. We provide our observations and analysis, note the lessons we have learned from recent experiences with clients, and offer examples that illustrate specific aspects of Section 404. We are pleased to share our experiences with you.

---

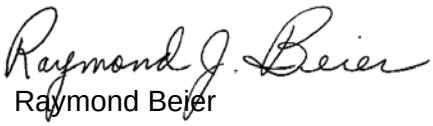
[1] Our previously issued white papers are entitled: *The Sarbanes-Oxley Act of 2002: Strategies for Meeting New Internal Control Reporting Challenges; The Sarbanes-Oxley Act of 2002 and Current Proposals by NYSE, Amex, and NASDAQ: Board and Audit Committee Roles in the Era of Corporate Reform;* and *The Sarbanes-Oxley Act of 2002: Understanding the Auditor's Role in Building Public Trust.* We have also issued a DataLine entitled, *Management's Responsibility for Assessing the Effectiveness of Internal Control Over Financial Reporting Under Section 404 of the Sarbanes-Oxley Act.*

PRICEWATERHOUSECOOPERS

Many companies have made significant progress in their efforts to comply with Section 404. For those companies this monograph should (i) provide useful perspectives on evaluating and testing the design and operational effectiveness of control over financial reporting that will be conducted in the future and (ii) affirm or initiate a reassessment of established work plans or processes. For other companies that are early in the process, this monograph should provide useful information in developing their overall strategy for implementing Section 404. It is worth noting that interpreting these new rules has proven to be an evolutionary process. Additional future interpretative guidance may be issued by the SEC for registrants and by the PCAOB for external auditors. Such guidance could impact views expressed in this publication.



Raymond Bromark
Americas Theater Leader
Professional, Technical, Risk and Quality



Raymond Beier
Leader
National Technical Services

Table of Contents

SECTION I: Executive Summary

The Most Significant Financial Legislation in Nearly 70 Years – Why the Sarbanes–Oxley Act Was Issued

The Public Company Accounting Reform and Investor Protection Act of 2002 (the Sarbanes–Oxley Act or the Act) was enacted in July 2002 largely in response to major corporate and accounting scandals involving several prominent companies in the United States. These scandals resulted in an unprecedented lack of confidence in the financial markets and a loss of public trust in corporate accounting and reporting practices. The Act has brought about the most extensive reform that the U.S. financial markets have seen since the enactment of the Securities Act of 1933 and the Securities Exchange Act of 1934.

The impact of the Act has been felt throughout the financial markets; every industry and service sector has been, and will continue to be, impacted. Section 404 of the Act, *Management Assessment of Internal Controls* (Section 404), which may be the most challenging aspect of the Act, requires most publicly registered companies and their external auditors to report on the effectiveness of the company's internal control over financial reporting. The obvious question is: How will companies implement Section 404?

This monograph explains the specifics of Section 404, delivers practical guidance on compliance, and provides realistic examples of the implementation issues that companies are facing. We also offer our perspective on many key issues.

The Benefits of Effective Internal Control over Financial Reporting

While some in the marketplace view the effort to comply with Section 404 as largely an administrative and compliance exercise; we encourage companies to consider this an opportunity to improve the effectiveness of their business processes. Key benefits of improved internal control over financial reporting include:

- improved effectiveness and efficiency of internal control processes
- better information for investors
- enhanced investor confidence

We acknowledge that these benefits do not come without cost. Many preparers have expressed concerns about the extent and complexity of efforts necessary to document, test, and evaluate their internal control over financial reporting wondering if the effort is worth the cost, both in terms of management time and fees paid to outside advisors.

However, we believe that effective internal control over financial reporting will have a positive impact on investor confidence in the markets. We expect that the requirements of Section 404 and the increased attention paid to corporate governance will encourage companies to enhance internal control and effect rapid remediation of any identified control deficiencies. These efforts should ultimately improve the quality of financial reporting, internally and externally.

Implications of Section 404

Section 404 poses significant challenges for corporate boards and management, including:

- the need to devote significant time and resources to ensure compliance

- the need for management to evaluate and report annually on the effectiveness of internal control over financial reporting
- the requirement for external auditors to opine on management's assessment of the effectiveness of its internal control over financial reporting
- the need to assess the implications of reporting this new information to the marketplace
- the need for board of director and audit committee oversight of management's process, findings, and remediation efforts as management scopes and executes its Section 404 plan

Preparing for management's assessment and the external audit of internal control over financial reporting requires a substantial investment of time, people, and intellectual capital. For example, 78 percent of the respondents to a recent PricewaterhouseCoopers survey of financial services executives indicated that they believe the overall effort of complying with Section 404 (i.e., planning, documenting, testing, etc.) is significantly greater than they had initially anticipated. We encourage management to consider the effort required to ensure compliance with Section 404 and take action now to rectify any resource shortfalls. We believe that successful implementation of the Section 404 mandate is a critical element in fully restoring investor confidence.

* * * * * *

The remainder of this monograph is segregated into the sections listed below. Each section includes observations and analysis, lessons we have learned, and frequently asked questions on a number of key issues involving management's responsibilities under Section 404. In addition, we have included the full text of answers to frequently asked questions recently published by the SEC staff and questions and answers that set forth the PCAOB staff's opinions related to the implementation of the PCAOB's Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction With an Audit of Financial Statements* (the Standard).

- Getting Started – Project Initiation
- Scoping and Planning – The Beginning of an Effective Project
- Use of Service Organizations
- Documentation – Evidence of Effective Internal Control
- Testing – Determining the Operating Effectiveness of Internal Control
- Evaluation of Internal Control Deficiencies and Reporting
- Communication – Important Observations
- Mergers and Acquisitions – Impact of the Sarbanes-Oxley Act

While much has been written about the Act and Section 404, very little existing information was designed to assist management in implementing an entire Section 404 compliance effort. This monograph is an attempt to fill that void. However, management should not consider this monograph a substitute for the SEC's final Section 404 rules, the Act, or the Standard. Rather, the monograph represents our perspectives on how companies might (1) approach their assessment of internal control over financial reporting and (2) address many of the implications emerging from this new reporting requirement.

SECTION II: Getting Started — Project Initiation

For most companies, undertaking a process to ensure compliance with Section 404 is likely to be significant and complex. The scope of the Section 404 assessment will extend well beyond a company's finance and accounting departments into major aspects of its information technology, tax, legal, and internal audit functions. Management also will have to coordinate extensively with third parties, including the external auditor and providers of outsourced services. While the task will be even larger in the first year, companies will have to comply annually.

This section highlights two areas, (1) project oversight and (2) project management, which we believe are important to ensure the success of a company's effort to comply with Section 404.

Project Oversight

A company's Section 404 project requires broad, senior-level oversight. Establishing accountability for every facet of the project and in every department and function involved will help make the project a success. Executive commitment and sponsorship are imperative for the following reasons:

- By its very nature, the project will impact many of the company's major departments and functions. Typically, the only common leader of these departments and functions is the chief executive officer.
- Some employees might otherwise perceive the compliance effort as concerning primarily the finance, accounting, or internal audit functions.
- Completion of the project will require a significant amount of time and company resources.

We have found that Section 404 projects are most successful when they are overseen, on a day-to-day basis, by the global controller or chief risk officer (or someone with an equivalent title) and are supported by the audit committee and senior management (principally the chief executive officer and chief financial officer). In some cases, these officers are heavily supported by the company's internal audit department. Although internal audit often provides the competency and objectivity that may be necessary in management's Section 404 assessment, management must recognize the importance of internal audit's traditional role and responsibilities in an organization. Management should assess the long-term sustainability of having internal audit personnel be the primary supervisors of the process. Senior management clearly has a stake in the project, since it has certified and will continue to certify its internal control under Section 302 of the Act, *Corporate Responsibility for Financial Reports* (Section 302), and will ultimately certify the Section 404 assessment. The key is to ensure that accountability for the project cascades down to the rest of the company.

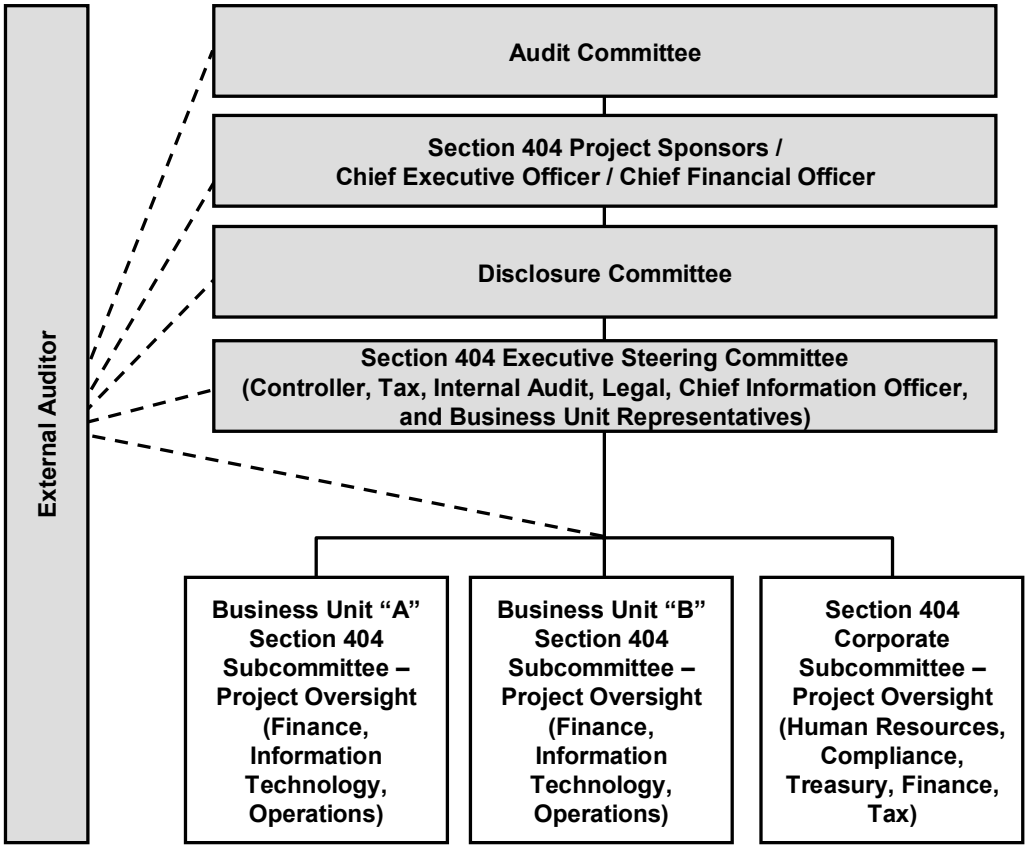
As it would in any high visibility project, senior management should clearly communicate its commitment as frequently as possible, including directly to the company's personnel or management teams, in intra-company newsletters, and in agendas for management meetings. Even more powerful than statements from the top is a visible demonstration of senior officers' commitment of top resources and funding to the project, as well as their time.

Sustainability of a company's efforts to achieve effective internal control over financial reporting is important. Compliance with Section 404 is much more than a one-time goal; it is a process that must be embedded in an organization. Thus, leadership's commitment must be sustained and continuous. While there are many ways

to achieve this, we recommend using an executive steering committee. This committee should have overall responsibility for the project's successful execution under the leadership of an executive sponsor. Similar to the composition of disclosure committees of many companies, the steering committee should have a representative from each key stakeholder group, typically including the finance, accounting, information technology, legal, and internal audit departments. At large companies with multiple business units or a wide geographic span, management may consider forming a series of subcommittees and have them report to the executive steering committee. The subcommittees should follow the company's organizational structure, whether delineated by business unit or geography. An example of a possible structure of these committees, for a company organized by business unit, follows:

External Auditor Interaction

To facilitate an open dialogue and timely identification and resolution of issues, participation by the external auditor in steering committee meetings is encouraged. The external auditor can also provide input on any new interpretive guidance issued by the staffs of the SEC or PCAOB.



Lessons Learned – Developing Internal Audit's Role

- *The company controller, chief risk officer, or compliance officer should take ultimate responsibility for the project, delegating tasks to other members of management who are accountable for the controls pertaining to specific processes.*
- *Although it is logical for internal audit to have significant involvement in the Section 404 project, it will also need to address other risks to the company that the project does not cover. If internal audit is responsible for the majority of the Section 404 project, the group's normal duties may go largely unaddressed.*

Before dedicating a substantial part of internal audit's time to the Section 404 project, a company should use a clearly defined process and a risk-based approach to reprioritizing the group's work. The original risk assessment that the company used to determine the scope of internal audit's responsibilities for the year should be re-evaluated in light of current needs surrounding the Section 404 project. Any changes in the plan should be agreed to by the appropriate stakeholders (e.g., the audit committee).

Accountability starts with the executive sponsor of the program. It is then delegated among various members of management throughout the company. Regardless of who documents an organization's processes and controls or who performs the testing for operational effectiveness, the person in charge of a particular process must take responsibility for his or her business processes and controls, ensuring that the control objectives are met. As management determines who is responsible for documenting and testing controls, it must evaluate the competence and objectivity of the individuals to ensure that sufficient assurance is obtained from the procedures performed.

Lessons Learned – Process Accountability

Typically, one of the weaknesses that companies first discover in their internal control is ambiguity about who is ultimately responsible for a business process from beginning to end. Often, business unit management believes that the finance/accounting organization is solely responsible for the financial reporting process. While this is true for certain processes, such as period-end financial reporting, much of the information in the financial statements originates outside the accounting/finance arm of a company. For example, the integrity of revenue reporting in the financial statements depends on the controls that are in place throughout the revenue process, starting with the initiation of the sale, continuing through the collection process, and ending with the general ledger entries.

While a company's finance organization may establish many of the policies for maintaining the integrity of financial reporting, the procedures and controls for complying with these policies are largely overseen by business unit management. For example, one of the key indicators of proper revenue recognition is an appropriately signed contract with the customer. Company policy should specify such indicators, but it is likely that the ultimate responsibility for seeing that those indicators exist lies with the company's sales organization, along with responsibility for the corresponding controls. Thus, not only is it important for a company to determine which key processes it will document and test, it is also important that management specify who is responsible for these processes and the controls related to financial reporting.

Frequently Asked Question (FAQ):
What role does the information technology organization play in a company's Section 404 project?

The information technology organization will have two primary roles in the project:

1. *To document and self-assess its own significant processes (referred to as general computer controls) for (a) the information technology control environment, (b) the development and implementation of information technology (program development), (c) a change to existing information technology (program changes), (d) information security (access to programs and data), and (e) computer operations. These are pervasive controls since the effectiveness of all automated controls across the organization depends on them.*

2. *To support personnel who are responsible for specific processes by helping those individuals document and assess their control activities. Because those individuals are accountable for the controls pertaining to the processes they oversee, they should be responsible for documenting and testing both manual and automated controls, even though automated controls often rely on or reside in information technology systems. It is important for personnel who are responsible for processes in their business units to understand all the controls for their processes, not simply the manual controls. To facilitate this understanding, the company should assign information technology liaisons to the control assessment teams.*

Project Management

A well-established framework for governing compliance with Section 404 will not, in itself, guarantee success. The project's success will also depend on strong execution, which in turn will largely depend on disciplined management of the project. Most companies will require full-time project management focus on the tools and methodologies associated with this discipline (i.e., developing and maintaining formal project plans, facilitating regular status meetings, and using a set of defined metrics to ensure rigor in the reporting to management). For a large, multinational company, a project support office may be required at each organizational unit. Although new project management teams may be assigned for the initial years of compliance, ultimately, a company should integrate compliance into its day-to-day operations.

In certain situations, a small or mid-size company will be able to manage its Section 404 project by relying on one or two individuals, depending on the company's complexity. These individuals should have full-time responsibility for the project. It is very difficult to manage the challenges of a Section 404 project on a part-time schedule.

Some may regard the creation of a separate department to manage compliance with Section 404 as resulting in unnecessary overhead, but many large companies will be required to coordinate perhaps fifty to one hundred teams worldwide, which will document thousands of control activities, and confront possibly hundreds of internal control deficiencies, many of which will require remediation. Without dedicated personnel with expertise in project management, Section 404 projects quickly can become overwhelming. Project management helps to:

- Establish and manage accountability across organizational units
- Ensure attainment of deadlines
- Develop consistent standards for documentation, testing, and reporting across organizational units

- Provide a mechanism to react to remediation requirements
- Provide a communication channel

Because no company is static, documentation and testing will need to be updated prior to the reporting date. Therefore, key to managing the Section 404 project is establishing an infrastructure and methodology for tracking and incorporating changes in internal control to ensure that the controls documented and tested by management represent those in effect as of the year-end date. Otherwise, management may inadvertently fail to test controls that have changed since its original assessment, which increases the risk that an internal control deficiency may exist but not be discovered or be discovered too late in the year for remediation prior to the reporting date.

SECTION III: Scoping and Planning – The Beginning of an Effective Project

Scoping involves determining the documentation necessary and the nature, timing, and extent of testing of controls to be performed for each significant account, disclosure, and business process at each of the company's locations. Scoping is one of the most critical phases in the Section 404 project. During this phase, management must identify the significant accounts, disclosures, and components; business processes/cycles and sub-processes/sub-cycles; and locations that will be subject to procedures. Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework. The Committee of Sponsoring Organization's (COSO) framework is the most widely applied model in the United States, and we recommend its use. This section is based on the assumption that companies will use the COSO framework.

FAQ: Can management use an internal control framework other than the COSO framework?

The SEC and PCAOB have acknowledged that other suitable frameworks have been published in other countries and new frameworks may be developed in the future. Currently, we believe that the use of a framework other than the COSO framework will be rare, given the widespread acceptance of the COSO framework.

This section provides an overview of how management should identify its significant accounts, disclosures, business processes/cycles, and locations that are subject to assessment. Then, specific scoping considerations are addressed as they relate to the five components of the COSO framework, (1) control environment, (2) risk assessment, (3) control activities, (4) information and communication, and (5) monitoring. Finally, the period-end reporting process, accounting judgments and estimates, general computer controls, and company-level controls warrant specific discussion and are covered later in this section.

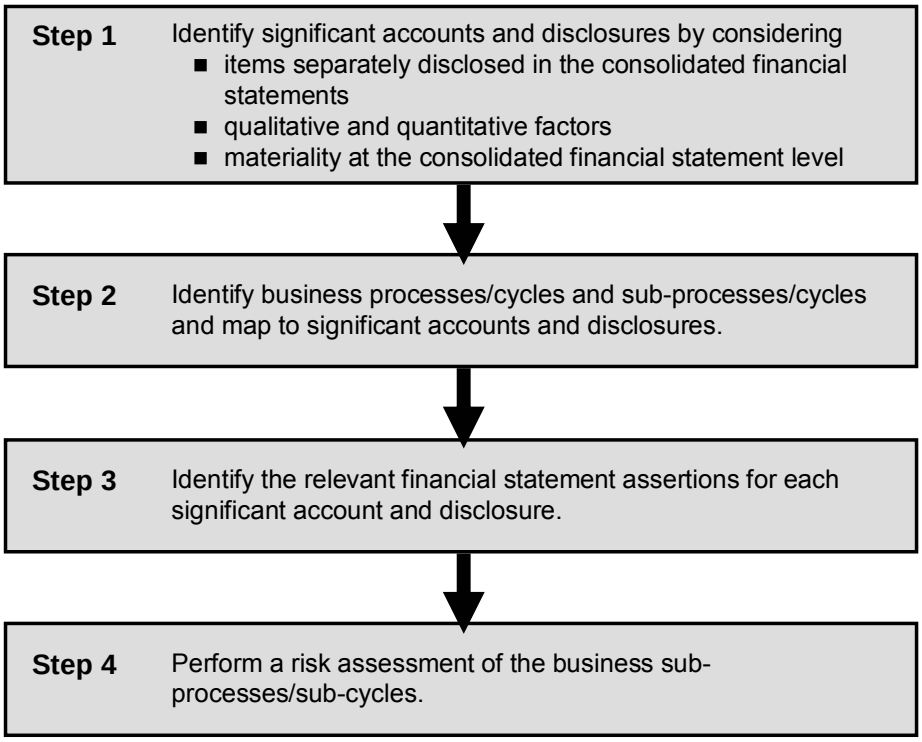
Significant judgment is involved in scoping decisions because of differences in companies' internal control and organizational structures. Management must maintain documentation to support each key decision. The format of the documentation will vary based on the complexities and size of the business. Examples of documentation methods are included in the appendices; however these templates are only examples of how management may document its scoping decisions. The use of memoranda (which is not among the examples) should also be considered.

External Auditor Interaction
We recommend that management meet with its external auditors on a regular basis to discuss the scoping process and key decisions made to date by management. These frequent meetings will avoid "surprises" and allow for effective and efficient execution and coordination between the parties.

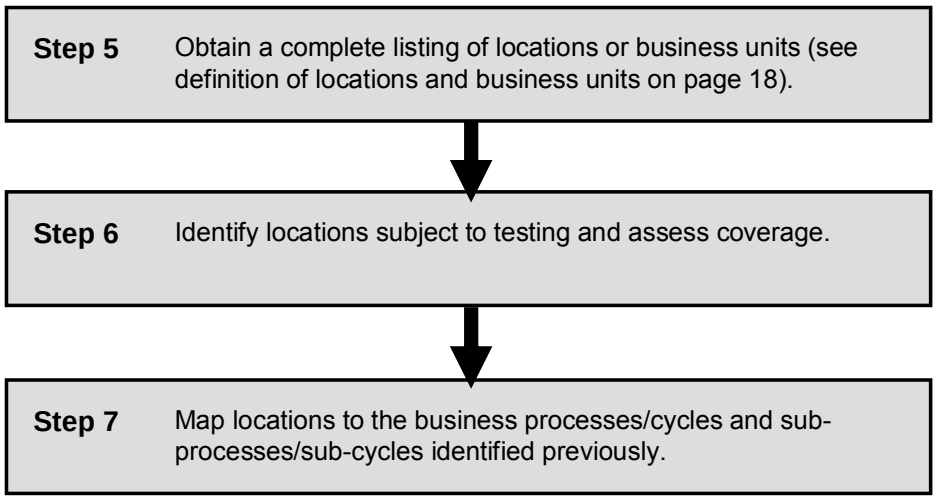
Although the objective of the scoping process is to identify the significant accounts, disclosures, business processes/ cycles, and locations that must be documented and tested, many different approaches may be taken to get to this end result. Although we will discuss the scoping process in a sequence of steps, they are inter-related and may be performed simultaneously. Management may identify significant accounts and map these accounts to the business processes/ cycles; alternatively, management may

begin the process by identifying the business processes/cycles. Regardless of the approach taken, the ultimate objective of the scoping exercise is the same.

Identify Significant Accounts, Disclosures, and Business Processes/Cycles

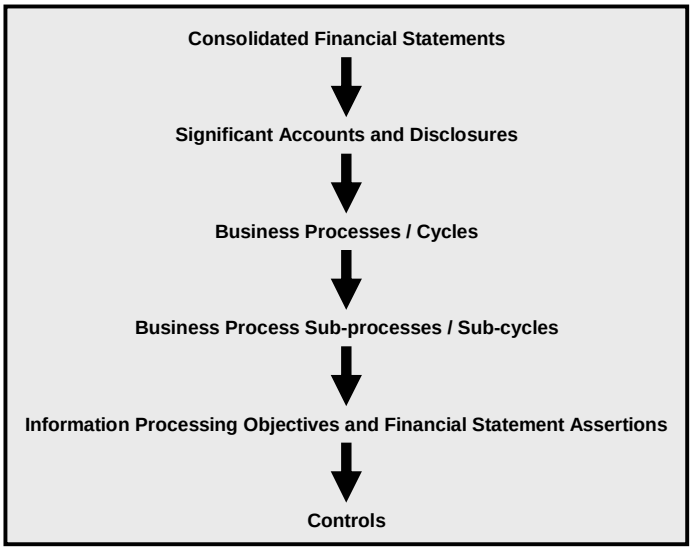


Determine Multiple-Location Coverage

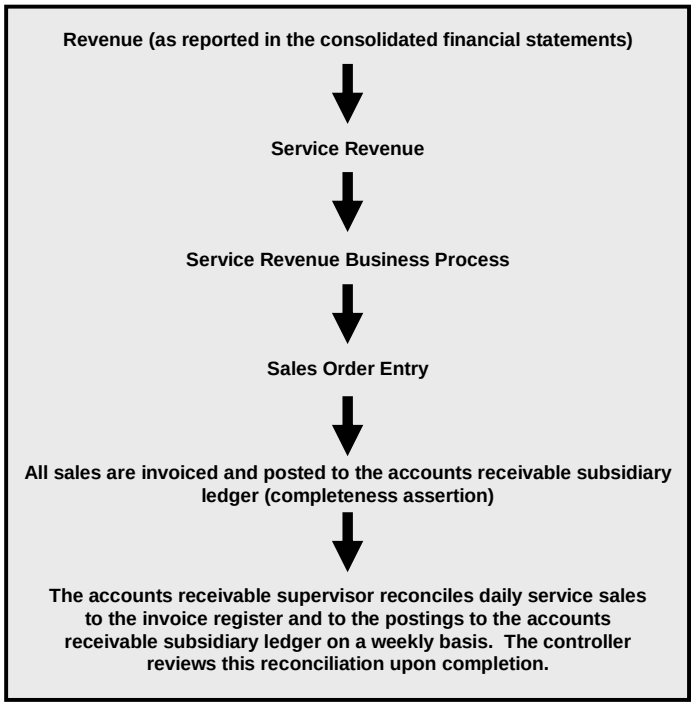


Identify Significant Accounts, Disclosures, and Business Processes/Cycles

One objective of the project is to determine the controls that address the relevant financial statement assertions for each significant account and disclosure in the company's external financial reports. To accomplish this objective, management should start with the consolidated financial statements and footnotes, and then move through each step, ultimately determining the internal control activities and procedures that address the relevant financial statement assertions. An illustration of this process follows.



An example of one aspect of the revenue cycle follows.



The steps in selecting the significant accounts, processes, and sub-processes, and linking them to management's assertions are further explained below.

Step 1: Identify significant accounts and disclosures by considering

- items separately disclosed in the consolidated financial statements
- qualitative and quantitative factors
- materiality at the consolidated financial statement level

Significant accounts and disclosures are identified at the (1) consolidated financial statement level and (2) individual account/component or disclosure level (e.g., inventory may comprise finished goods, work-in-process, and raw materials, or revenue may comprise product revenue and service revenue). The Standard indicates that an account or disclosure is significant if there is a more-than-remote likelihood that the account could contain misstatements that, individually (or when aggregated with other misstatements), could have a material effect on the financial statements (as a result of either overstatement or understatement). The notion of "significance" should not be based solely on a quantitative measure. Certain accounts may be significant on a qualitative basis or because they represent an important performance measure to investors.

For purposes of determining significant accounts, management should assess the likelihood of a misstatement without giving any consideration to the effectiveness of internal control over financial reporting. Qualitative determinations about significance depend on subjective reasoning. We have provided general guidelines in the following paragraphs that may clarify the assessment process.

The accounts and disclosures that are presented in the published financial statements and footnotes filed with the SEC represent the starting point for determining which accounts are significant. We believe that management should consider the following key points when assessing significance:

- There is a presumption that, taken as a whole, all line items and footnotes (e.g., pension or postretirement benefits, income taxes, and segment data) in the published financial statements are significant. However, if the financial statements are highly disaggregated, typically management should presume that all consolidated balance sheet and income statement account balances/components that are greater than management's planning materiality threshold are significant. (Planning materiality is discussed below.)
- Accounts that may not be significant at a particular time but undergo significant activity (e.g., cash flow) or have exposure to unrecognized obligations (e.g., loss reserves and other liability accounts) generally would also be considered significant. For example, the Standard indicates that loss reserves related to a self-insurance program may have historically been insignificant in amount, yet might represent a more-than-remote likelihood of material misstatement due to the existence of material unrecorded claims.

FAQ: Because management's assertion must be as of the company's most recent fiscal year-end, does management have to revalidate its initial scope assessment throughout the year?

Yes. It is important that management implement a process for regularly reassessing its initial scoping decisions to ensure that they are appropriately updated for significant business changes. Because scoping decisions are made early in the process, it is likely that certain aspects of those decisions will change as the year progresses. Factors that may impact scoping decisions include:

- *Acquisitions and divestitures*
- *Changes in expected or budgeted financial results that were initially used to determine significant accounts and locations subject to review*
- *Determination of specific risk areas at a location*
- *Changes in management at an individual location*
- *Identification of internal control deficiencies*
- *Inadequate company-level controls*

Quantitative Considerations

In order to determine which accounts are significant, management must consider the concept of materiality. The same definition of materiality that applies to the preparation of financial statements applies to planning and reporting the effectiveness of internal control over financial reporting. Materiality is more than just a quantitative concept; judgments about materiality are subjective and may change throughout the process. Management must make its own materiality decisions.

The concept of materiality is applied to the consolidated financial statements and to individual accounts/components. We believe management should consider the following criteria for determining the scope of its internal control testing:

Overall materiality: Overall materiality involves the risk of material misstatement of the consolidated financial statements. Management should consider the guidance included in SEC Staff Accounting Bulletin No. 99, *Materiality*, when assessing materiality. Applying a materiality threshold (e.g., 5 percent) against certain key metrics, such as pre-tax income, is useful for making a preliminary assumption about whether an item is likely to be material. Additionally, overall materiality is used to assess whether aggregated misstatements at the level of an individual significant account (and, similarly, the aggregated deficiencies in an audit of internal control) are material to the consolidated financial statements.

Planning materiality: We believe planning materiality is typically based on an income statement measure, such as pre-tax income (loss), and should be used to determine the significance of individual accounts (or components of accounts). To provide an allowance for the aggregation of misstatements across individual accounts and for detection risk (the risk that controls will fail to detect a material misstatement), planning materiality should be less than overall materiality.

We believe planning materiality generally to range between 50 and 75 percent of the overall materiality based on the level of risk (i.e., a higher risk entity would have a lower planning materiality, and a lower risk entity would have a higher planning materiality). For example, if the overall materiality is $1 million of pre-

tax income (loss), planning materiality for a higher risk entity might be $500,000 (i.e., 50 percent of $1 million), and planning materiality for a lower risk entity might be $750,000 (i.e., 75 percent of $1 million).

Overall materiality and planning materiality levels should be documented, along with (1) the rationale behind the quantitative materiality levels and (2) any changes in the determination of materiality that arise during the remainder of the project.

When identifying significant accounts, management must disaggregate the financial statement line items and footnote disclosures to determine whether any comprise multiple accounts or components that may also be individually significant. For example, the "other current assets" line item on the consolidated balance sheet may include multiple accounts or components that may be derived from separate classes of transactions and thus be subject to different risks or controls. In this case, these accounts/components should be assessed separately. If any of these components exceed the planning materiality threshold, we believe it should be considered significant, even though it is not separately disclosed in the financial statements. Other examples include:

- Revenue streams having different characteristics (e.g., product revenues versus service revenues)
- Different components of inventory (e.g., raw materials, work-in-process, and finished goods)
- Contract-driven service fees versus expenses for materials and supplies

Qualitative Considerations

The Standard indicates the following examples of qualitative factors that should also be considered when assessing the significance of an account:

- Composition of the account
- Susceptibility to loss due to errors or fraud
- Volume of activity, complexity, and homogeneity of the individual transactions processed through the account
- Nature of the account (for example, suspense accounts generally warrant greater attention)
- Accounting and reporting complexities associated with the account
- Exposure to losses represented by the account (for example, loss accruals related to a consolidated construction-contracting subsidiary)
- Likelihood (or possibility) of significant contingent liabilities arising from the activities represented by the account
- Existence of related-party transactions in the account
- Changes in account characteristics since the previous period (for example, new complexities, subjectivity, or types of transactions)

Management should consider all of the aforementioned factors when deciding whether to include or exclude specified accounts in its assessment.

FAQ: What should be included within the scope of management's Section 404 assessment?

The assessment covers the financial statements and related footnotes. Additionally, we believe the financial statement schedules (e.g., schedule of valuation and qualifying accounts) required to be included in Form 10-K should be covered in management's assessment of internal control over financial reporting. We believe this position is supported by the fact that an alternative form of reporting accepted by the SEC is to include such information in the notes to the financial statements rather than in separate financial statement schedules.

Additionally, the PCAOB staff has indicated that the Standard's reference to financial statements and related disclosures does not extend to the preparation of Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A) or other similar financial information presented outside of the company's financial statements and footnotes (refer to Question 5 in Appendix IX for further clarification included in the PCAOB staff's FAQs). However, because some of the financial information included in MD&A is derived directly from the financial statements, we believe management should have a process to ensure that information in MD&A is consistent with the information in the financial statements.

Step 2: Identify business processes/cycles and sub-processes/cycles and map to significant accounts and disclosures.

Next, management determines the company's significant business processes/cycles and sub-processes/ sub-cycles that generate the significant accounts. Examples of common processes/cycles and sub-processes/ sub-cycles are provided in Appendix I. We believe that the business processes/cycles are the foundation for the internal control assessment. By understanding and documenting the business processes/cycles, management is able to identify the control activities that address the information processing objectives/CAVR (completeness, accuracy, validity, and restricted access), as well as potential "gaps" in the controls (i.e., information processing objectives for which control activities are not in place). See Definition of Key Terms at the end of this monograph for further discussion of information processing objectives/CAVR.

Mapping is an exercise performed to link significant accounts to the business processes/cycles or sub-processes/ sub-cycles that generate them. Mappings are useful to ensure that all significant accounts have been addressed by a business process/cycle and that all significant business processes/cycles have been identified. If management fails to identify all of the processes, it will be more difficult to determine the corresponding control activities that address each relevant assertion. Within each business process and sub-process, management determines which control activities address the information processing objectives/CAVR over the significant accounts. Appendix II and Appendix III include examples of how the financial statement accounts could be mapped to the cycles.

Significant business processes/cycles and business sub-processes/sub-cycles will vary by entity. For example, research and development or advertising and promotion expenditures may be significant to a consumer products company but not to a financial services company.

Lessons Learned – Prioritization

We have found that management spends the majority of its time on routine/transactional processes and control activities. However, management must also focus on accounts that are most susceptible to material misstatement. Often these accounts are not transactional but rather, non-routine accounts that involve significant judgment and estimation.

Step 3: Identify the relevant financial statement assertions for each significant account and disclosure.

For each significant account and disclosure, management should identify and document relevant financial statement assertions, as well as test the controls that apply to those assertions. The Standard describes the nature and provides examples of the following five assertions:

- existence or occurrence
- completeness
- valuation or allocation
- rights and obligations
- presentation and disclosure

Descriptions and examples of each assertion are included in the Definition of Key Terms at the end of this document. The PCAOB staff has indicated (refer to Question 10 in Appendix IX) that management may base its evaluation on assertions that differ from the five specified in the Standard.

The Standard indicates that relevant assertions are assertions that have a meaningful bearing on whether the account or disclosure is fairly stated. The degree to which an assertion is relevant to each significant account will vary. For example, assertions about valuation may not be relevant to the cash account unless currency translation is involved; however, assertions about existence and completeness are always relevant. Additionally, management may focus on assertions about presentation and disclosure separately, in connection with the period-end financial reporting process. In determining whether a particular assertion is relevant, management should consider:

- The nature of the assertion
- The volume of transactions or data related to the assertion
- The nature and complexity of systems, including information technology systems that the entity uses to process and control information that supports the assertion

Management should determine relevant assertions prior to testing to minimize the likelihood of testing controls that address assertions that are not relevant to a particular significant account.

Although the financial statement assertions appear to be similar to the information processing objectives/ CAVR, there is not a one-for-one relationship, and they are used for different purposes. Information processing objectives/CAVR are used to evaluate the design effectiveness of controls, particularly application controls, within a business process. Financial statement assertions are representations by management as to the fair presentation of the financial statements.

FAQ: Why is it beneficial to address the information processing objectives/CAVR (completeness, accuracy, validity, and restricted access) at the transaction level for each business process?

Until management understands the controls within the business processes/cycles that generate the account, it may be difficult for management to determine the effectiveness of controls for an account. By testing a control activity only at the level of the financial statement assertion, management might not determine to its satisfaction that (1) controls are in place for the input, processing, and recording of the data underlying the financial statement component and (2) the entire control system for that business process is in place and functioning as intended.

Step 4: Perform a risk assessment of the business sub-processes/sub-cycles.

The next step in the scoping process is to identify the risks within the sub-processes/sub-cycles that may result in a material misstatement in the financial statements. The risk assessment will be used to assess the nature, timing, and extent of the testing that must be performed in each area. For example, at some companies, fixed asset balances may be significant; however the balances are less judgmental in nature and thus are of lower risk. In these cases, testing of the control activities that support the processes around capital spending may be performed earlier in the year or the extent of testing may be reduced. The risk assessment requires significant judgment and should be performed by members of management that have sufficient knowledge of the processes and associated risks. As with the determination of significant accounts, qualitative and quantitative factors must be considered. Various methods may be used to perform the risk assessment. Management should determine its strategy for assessing the risk for each process/cycle and ensure that its methodology is consistently applied and sufficiently documented.

An example of a process for risk assessment and related documentation is in Appendix IV.

Determine Multiple-Location Coverage

In cases where the business processes/cycles and sub-processes/sub-cycles take place at multiple locations (i.e., corporate offices, manufacturing plants, distribution centers), management must decide which locations will be included in its internal control assessment. The Standard refers to these locations as “individually important” or “financially significant” (these terms will be used interchangeably in this document). In addition to individually important locations, management will need to perform certain procedures at locations with specific risks and locations that are not individually important, but that may be significant when aggregated with other locations. The Standard includes a general decision tree (see page 18) that directs the reader through this decision process. However, management’s approach will depend on how the company is organized.

Management must decide which locations or business units should be included in its assessment by evaluating factors such as

- the relative financial position and operations of the location/business unit
- the risk of material misstatement that the location/business unit poses
- the extent to which business processes/cycles and underlying controls for a given location/business unit are part of a central-processing or shared-services environment

Ultimately, controls will be identified and tested at the location that is responsible for implementing them.

Step 5: Obtain a complete listing of locations or business units.

When determining the locations or business units (the terms location(s) and business unit(s) are used interchangeably in this document) that are subject to assessment, management should identify all locations. Although this may seem like a straightforward task, it may prove challenging for many multinational organizations, because of their complex organizational structures.

Equity Method Investments

The SEC staff's FAQs (refer to Question 2 in Appendix VIII) indicate that controls over the recording of transactions into the investee's accounts are not part of the registrant's internal control structure. However, the evaluation of a company's internal control over financial reporting should include the company's own controls for reporting the equity method investment (including the investee's earnings/losses) and making the related disclosures in the investor's financial statements, in accordance with generally accepted accounting principles (GAAP).

Variable Interest Entities and Proportionately Consolidated Entities

In its FAQs (refer to Question 1 in Appendix VIII), the SEC staff has indicated that management may exclude an entity from its assessment in situations when:

- the entity was in existence prior to December 15, 2003 and is consolidated by virtue of FASB Interpretation No 46, *Consolidation of Variable Interest Entities,* and
- the registrant does not have the right or authority to assess the internal controls of the consolidated entity and also lacks the ability, in practice, to make that assessment

Similarly, entities accounted for via proportionate consolidation in accordance with EITF 00-1, *Investor Balance Sheet and Income Statement Display Under the Equity Method for Investments in Certain Partnerships and Other Ventures,* where management has been unable to assess the effectiveness of internal control at those entities due to the inability to dictate or modify the controls of the entities and the inability in practice, to assess those controls, may be excluded from management's assessment.

The Standard provides that if management limits the scope of its assessment, the external auditor may limit its audit in the same manner, however the auditor should include in its report discussion of the exclusion of an entity from the scope of both management's assessment and the auditor's audit of internal control over financial reporting (refer to Question 19 in Appendix IX).

FAQ: What is the definition of a location or a business unit?

The definition of a location or a business unit depends on the nature and organizational structure of the company. A business unit may be a legal entity (e.g., subsidiary), a division, or an operational facility (e.g., a plant or sales office). Management must use significant judgment when defining a location or a business unit for scoping and testing purposes. The objective in the selection of locations is to ensure that the controls are assessed and tested at the level at which they are performed. Any or all of the following factors may play a role in determining how a location or a business unit will be defined for scoping and testing purposes:

- *Sources of available financial information (e.g., a legal entity, business unit, plant, or sales office)*
- *Extent of centralized processes/shared-accounting services within various levels of the company*

FAQ: What is the definition of a location or a business unit? *Continued*

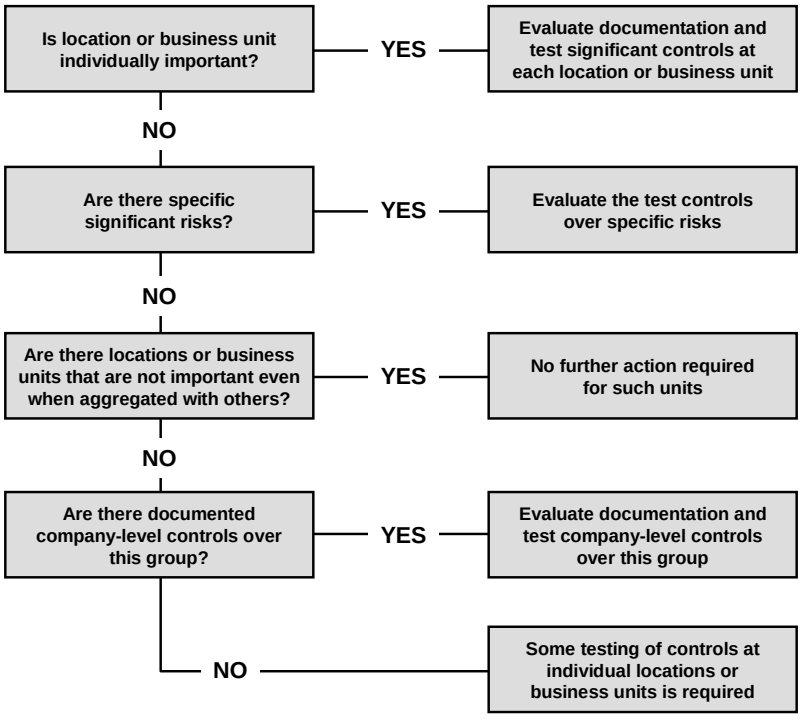
- *Geographic organization*
- *Legal structure*
- *Management structure/hierarchy*
- *Existence of equity method investments*
- *Entities consolidated under FIN 46*

Evolution of the company (e.g., recent growth through acquisitions and/or organic growth; recent or planned internal reorganizations; disposition or dissolution of an operation)

Step 6: Identify locations subject to testing and assess coverage.

To determine which locations must be included in the company's assessment of internal control over financial reporting, management should evaluate each location's relative financial significance and the risk of material misstatement associated with that location. To evaluate the significance of each location, management should prepare financial information by location; the information should be reconciled with reported balances to ensure completeness. For locations that are individually important (defined in Step 6A below), management should document and test controls for all significant accounts and disclosures. Generally, a relatively small number of locations or business units will encompass a large portion of a company's operations and financial position, making them financially significant. However, if management cannot test a large portion of the company's operations and financial position by selecting a relatively small number of locations, management must select additional locations or consider whether a sampling technique may be appropriate (refer to the FAQ on page 22). Testing company-level controls is not a substitute for testing controls for a large portion of the company's operations or financial position.

The Standard includes the following decision tree to illustrate the steps that should be taken in this categorization process:



6A. Determine which business units/locations are individually important.

The goal of this step is to determine which locations are individually important (financially significant) and thus yield sufficient coverage using meaningful quantitative metrics (reflective of the company's specific risks). Although the PCAOB has not established specific percentages to determine coverage (refer to Question 17 in Appendix IX), we believe sufficient coverage involves obtaining at

least 60 to 70 percent of the company's operations and financial position (including individually important locations and the specific risk areas discussed in Step 6B). Ideally, these locations will represent a relatively small number of the company's locations. Individually important locations are generally those meeting at least one of the balance sheet or one of the income statement consolidated metrics that are shown below. The suggested maximum consolidated metrics to be used for selecting individually important business units/locations are as follows:

- > 5 percent of annual revenues
- > 5 percent of pre-tax income
- > 5 percent of total assets
- > 5 percent of equity (if applicable)

These metrics may need to be adjusted to take into account different organizational structures. For example, if a company operates in a decentralized manner with multiple, similarly sized business units, the percentages that it uses to determine individually important locations may need to be reduced to 1 or 2 percent of the indicated metrics to obtain sufficient coverage.

The quantitative metrics should be derived from the consolidated financial statements filed with the SEC. When identifying individually important locations, many companies have used financial information from the most recent fiscal year-end (e.g., the consolidated statements dated December 31, 2003) or quarter-end. However, the financial information that management uses in this analysis may vary with the level of detailed financial information available and the reliability of the data (e.g., annual vs. quarterly vs. monthly results). Ultimately, management should use the financial information that it considers most representative of the company's fiscal year-end under assessment. The source of information may include the following:

- Detailed company annual budgets by location for the fiscal year-end under assessment
- The most recent fiscal year-end results
- A combination of recent quarterly data (for the balance sheet) and the most recent fiscal year-end data (for the annual income statement) ─ for example, a company with a December 31, 2004 year-end may use the quarter that ended on March 31, 2004 for balance sheet data and the year that ended on December 31, 2003 for income statement results

If the financial results that management has chosen as the source information have been substantially impacted by unusual events or significant transactions, management should modify the results so that they do not reflect those events and transactions. Any budget or prior year data should also be updated to reflect any significant anticipated changes.

After identifying individually important locations based upon the selected metrics, management should assess coverage. As indicated, we believe coverage over at least 60 to 70 percent of the consolidated metric should be obtained (including those specific risk areas discussed in Step 6B).

FAQ: A registrant has a large subsidiary that it intends to sell completely by the end of its second quarter. The subsidiary is not itself a registrant. Is there any reason to test the controls at the subsidiary for purposes of the registrant's year-end Section 404 assessment? Additionally, how should management assess a component of the business that is reported as a discontinued operation at year-end, but is not sold until after year-end?

In relation to the sale prior to year-end, management may not need to test controls at the subsidiary for purposes of the registrant's year-end Section 404 assertion, unless there is a chance that the sale transaction will not be completed as planned.

In the case of a discontinued operation, the Standard requires that an operation that is accounted for as a discontinued operation on the date of management's assessment (i.e., year-end) be included in the scope of the evaluation of the company's internal control. The closing date of the sale determines whether a discontinued operation is within the scope of the internal control evaluation. If the sale closes before the date of management's assessment, there is no need to test controls for the discontinued operation as part of the assessment of internal control over financial reporting. If, however, the sale were to close after the date of management's assessment, the discontinued operation would be within the scope of the company's internal control assessment, regardless of the timing of the Form 10-K filing.

FAQ: How should management select the quantitative measure that will be used to identify individually important locations?

The quantitative measure should be tailored to the company. For example:

- *Pre-tax income may not be a meaningful metric if the company has breakeven results or if there are significant intercompany charges among the locations.*
- *Equity may not be a meaningful metric if the balance at the location or business unit level comprises primarily intercompany account balances or if headquarters records significant "top level" adjustments in equity during the consolidation process (e.g., eliminates an acquired subsidiary's pre-acquisition equity).*
- *Total assets may be the most relevant balance sheet metric for a manufacturing company with significant amounts of inventory, receivables, and fixed assets.*

At a minimum, we believe management should use ***one balance sheet metric (e.g., total assets or equity) and one income statement metric (e.g., revenue or pre-tax income)*** *in connection with the quantitative assessment. For example, using pre-tax income and total assets as quantitative measures would be acceptable; however, using total assets and total equity would not be acceptable.*

Management should document the rationale for the appropriateness of the selected financial metrics.

FAQ: Is the company required to test the design and operating effectiveness of internal control over financial reporting at all individually important locations, even if the company can achieve a large portion of coverage without visiting all individually important locations?

Yes. We believe the Standard requires that the design and operating effectiveness of internal control over financial reporting be tested at all individually important locations even if the company can obtain a large portion of coverage without including an individually important location. For example, assume that a company has locations that represent the following percentages of pre-tax income and total assets:

Location A	*30%*
Location B	*20%*
Location C	*15%*
Location D	*10%*
Location E	*10%*
Location F – M	*Each less than 5%*

Based on these facts, testing of the design and operating effectiveness of internal control over financial reporting for all significant accounts and disclosures should be performed at locations A, B, C, D, and E despite the company's ability to obtain 65 percent coverage from locations A, B, and C. This is because location D and E are individually important.

FAQ: How should management determine which locations are individually important if a particular location has multiple operating facilities?

For most companies, using segment data or reporting unit data for this scoping exercise will not be an appropriate or efficient approach, since management must ultimately determine which operating units are actually conducting the control activities and processes that need to be tested. It may be preferable to disaggregate the financial data, and then use the lowest level data as the basis for selecting individually important locations. In this situation, the quantitative factors determining the selection of individually important locations may need to be reduced, or the desired coverage might not be obtained. ***When calculating the overall quantitative coverage, management should consider only those locations (e.g., the operating facilities in this example) that are subject to testing.*** *For example, assume a business unit with 20 manufacturing plants is identified as being an individually important location, and management plans to visit 12 of the 20 plants. In this case, management would only consider the coverage obtained from these 12 plants, and not the entire business unit. Management may opt to further disaggregate its business units when selecting individually important locations.*

FAQ: How should management identify individually important locations when the company has numerous, similar-sized locations?

When a company has numerous locations that are the same size and are not individually important, management may obtain very little coverage when using the quantitative metrics and identification of specific risk areas. For example, assume a company has one centralized shared-services center that processes transactions for its 100 plant locations (none of which are individually important). In addition, assume that the 100 plant locations use a common set of processes.

In this case, the plants are responsible for providing complete, accurate, and valid inputs to the shared-services center. For example, the shared-services center may match the receiving document, the purchase order, and the invoice prior to making payments on behalf of the 100 plant locations. The merchandise is received at the plant locations and this three-way match control is dependent upon accurate, valid, and complete receiving information. Therefore controls over the receiving of the merchandise at the plants would need to be tested to ensure the three-way match control is operating effectively. Assuming the controls over receiving of merchandise are common across all locations, we currently believe it would be acceptable for management to sample the locations for testing of the inputs into this process. In addition, management needs to evaluate the controls at the shared-services center. Using this approach, management normally would be obtaining coverage over a large portion of the company's operations and financial position.

The PCAOB staff's FAQs (refer to Question 18 in Appendix IX) provide support that sampling may be used by the auditor for entities with a large number of individually insignificant locations, assuming the sample is representative of the entire population and there is an expectation of no or very few exceptions. However, if a company has numerous similar-sized locations, but does not have shared-services or common processes and controls, we currently believe management should obtain sufficient evidence to conclude that controls are operating effectively at locations representing a large portion of a company's operations or financial position. Management should continue to monitor practice in this area as it evolves.

FAQ: When locations are deemed individually important, what must management test at those locations?

At a minimum, management should test controls over all relevant assertions for each significant account balance or disclosure at an individually important location for which the selected accounts are material at the location. Additionally, management would test company-level controls from two perspectives:

1. *The perspective of the location — What are the control environment, risk assessment, information and communication, and monitoring functions specific to the location?*
2. *The perspective of looking "upward" regarding controls directed by corporate headquarters — Management should ensure that company-level controls are working according to their design (i.e., the corporate accounting policy manual is being used at the location).*

The PCAOB staff has further clarified in its FAQs (refer to Question 16 in Appendix IX) that a significant account (at the consolidated financial statement level) at an individually important location need not be tested if it is immaterial at that location. However, if an account is material at a location that is not individually important, the controls over all relevant assertions for that account should be tested. See Step 6B for discussion of the identification of specific risks.

6B. With respect to the remaining locations, determine whether there are specific significant risks in specific areas.

Even though a location's relative financial significance to the consolidated financial position or operations may be small, the location may still be responsible for certain areas that expose the entity to the risk of a material misstatement. For locations carrying specific risks (e.g., a location responsible for foreign exchange trading or treasury operations) that could result in a material misstatement, management should document and test controls that mitigate those specific risks, as well as document its rationale for categorizing certain factors as specific risks.

Examples of factors that may indicate increased risk in an area at a location include

- Management's risk assessment
- Internal or external audit findings and recommendations
- Significant, unusual, or non-recurring transactions
- Significant individual account balances
- Changes in management

Specific risk locations contribute to the consolidated coverage of the selected quantitative metrics when the accounts affected by the specific significant risk are directly included in the selected metrics. For example, if the specific risk and the selected income statement metric are both revenue, the revenue from the specific risk location would be included in the coverage calculation. However, if the income statement metric is pre-tax income and the specific risk is revenue, the pre-tax income from the specific risk location would not be included in the calculation of coverage of the pre-tax metric.

FAQ: What should be done if the individually important and specific risk locations do not provide management with the appropriate coverage?

In this case, management should:

- *re-evaluate the specific risks and ensure all have been identified*
- *re-evaluate and lower the quantitative metrics used to identify the individually important locations to select additional locations to obtain the necessary coverage*

If lowering the selected metrics results in additional locations that bring total coverage to an amount more than is necessary, all locations that meet this lower threshold still should be included (i.e., management cannot select only some of the individually important locations that represent more than the selected metric to arrive at coverage of 60 to 70 percent). If lowering the quantitative metrics does not result in a sufficient coverage due to numerous small similar-sized locations, reference should be made to the FAQ on page 22.

6C. If the remaining *aggregated* locations are insignificant and thus could not result in a material misstatement to the financial statements, no further procedures are necessary.

With respect to locations that cannot cause, either individually or in the aggregate, a material misstatement in the company's financial statements, management need not perform procedures at those locations. We believe

that the aggregate of these individually unimportant locations would typically be less than five percent of the quantitative thresholds for the individually important locations and that none would have specific qualitative risks.

6D. If the remaining locations are significant when aggregated, management will need to consider the following:

1. If company-level controls are effectively designed and operating, management should obtain assurance through documentation and testing of company-level controls. In addition, management may determine that other evidence is necessary.

2. If company-level controls are *not* effectively designed or operating, management must perform testing of control activities at these locations in order to obtain the necessary assurance that such controls are designed and operating effectively.

If company-level controls are in place, management should document and test them. To conclude that company-level controls are operating effectively at these locations, management ordinarily would need to visit at least some of the locations and assess that the controls are operating effectively. In addition, management may determine that evidence such as walkthroughs, self-assessments, internal audit reviews, or monitoring controls is necessary to conclude that control activities at these locations are designed and operating effectively.

If (1) the company does not have company-level controls in place at these locations or (2) the controls are not reliable, management will need to determine the nature, timing, and extent of the procedures to be performed at each location to obtain the necessary assurance. (Company-level controls are discussed later in this section.)

In evaluating which locations should undergo company-level control testing and the controls to be tested, the Standard indicates the following factors should be considered:

- The relative financial significance of each location
- The risk of material misstatement arising from each location
- The similarity of business operations and internal control over financial reporting at the various locations
- The degree to which processes and financial reporting applications are centralized
- The effectiveness of the control environment, particularly management's direct control over the exercise of authority delegated to others and its ability to supervise activities effectively at the various locations
- The nature and amount of transactions executed and the related assets at the various locations
- The potential for material unrecognized obligations at a location and the degree to which a location could create an obligation on the part of the company
- Management's risk assessment process and analysis for excluding a location from its assessment of internal control over financial reporting

FAQ: Is it necessary to obtain a large portion of coverage at the individual account level?

Typically, we believe that coverage of 60 to 70 percent of the selected consolidated metrics (i.e., total revenues, total assets, total equity, or total pre-tax income) will translate into coverage of approximately 60 to 70 percent at the level of a significant account or disclosure. In some situations, coverage of a significant account or disclosure will fall below 60 percent. As indicated in the Standard, a large portion of coverage is determined at the overall financial statement level not an individual account level. As a result, the company is not required to add more locations in order to attain a minimum coverage level of 60 percent for all significant accounts and disclosures. However, it will be important for management to exercise judgment in these situations. We believe that if the coverage of a significant account or disclosure is below 50 percent, management should reassess its identification of specific significant risks and consider selecting additional locations to gain sufficient evidence of the operating effectiveness of the controls related to that account or disclosure. Substantially low coverage (below 50%) may indicate that a specific significant risk has been overlooked in the initial scoping process. The PCAOB staff's FAQs (refer to Question 16 in Appendix IX) require the auditor to test controls over all relevant assertions for significant accounts that are material at locations that are not otherwise considered financially significant.

Step 7: Map locations to the business processes/cycles and sub-processes/sub-cycles identified previously.

The next step is to document and test of controls within the sub-processes/sub-cycles at each location. For example:

- A manufacturing plant may be responsible only for the controls covering the receiving and inventory production sub-processes/sub-cycles.
- A distribution center may be responsible only for the controls covering the sub-processes/sub-cycles of inter-company transfers and shipping.
- The corporate division of a company may be responsible for payroll processing, treasury activities, and purchasing on behalf of multiple locations.

Appendices II and III include examples of how mappings of significant accounts, cycles/processes, and sub-cycles/sub-processes may be performed and documented.

Recap for Determining Multiple-Location Coverage

Minimum Account Balance Coverage	Location	Planned Procedures
60 – 70%	Individually important locations and Accounts with specific risks	Detailed evaluation and tests of controls over significant (or "specific risk") accounts and disclosures at that location and testing of company-level controls.

Minimum Account Balance Coverage	Location	Planned Procedures
25 – 35%	Locations considered important when aggregated	Evaluate and test company-level controls, if applicable, and consider obtaining other evidence or perform some tests of controls at locations if company-level controls do not exist.
<5%	Immaterial locations, individually and in the aggregate	No testing required.

The Five Components of Internal Control

As part of management's Section 404 assessment, it must document, test, and evaluate the five components of internal control. These components are discussed below.

Control Environment

The control environment establishes the overall tone for the organization and is the foundation for all other components of internal control. COSO identified seven sub-components of the control environment:

- Integrity and ethical values
- Commitment to competence and development of people
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resources policies and procedures
- Participation by those charged with governance (i.e., board of directors, audit committee)

Examples of factors that management should consider when evaluating its control environment:

- Management's specification of the level of competence needed for particular jobs and the ultimate fulfillment of those specifications
- Management's (1) conveyance that integrity and ethical values cannot be compromised and (2) assurance that employees will receive and understand that message.
- Management's continuous demonstration, through words and actions, of a commitment to high ethical standards
- A philosophy and operating style of management that have a pervasive, positive effect on the entity.
- An organizational structure that is not so simple that management cannot adequately monitor the entity's activities nor so complex that the structure inhibits the necessary flow of information.

- Executives that fully understand their control responsibilities and possess experience and levels of knowledge requisite to and commensurate with their positions
- The assignment of responsibility, delegation of authority, and establishment of policies that (1) provide a basis for accountability and control and (2) set forth employees' respective roles and responsibilities in the organization
- Human resource policies that are central to recruiting and retaining competent people who will enable the entity to carry out its plans and achieve its goals

The Standard specifies that management must also address anti-fraud programs and the effectiveness of the audit committee when evaluating the control environment.

Anti-Fraud Considerations

The Standard indicates that all controls should be evaluated that are intended to address the risks of fraud and have at least a reasonably possible likelihood of having a material effect on the company's financial statements. We believe effective anti-fraud program includes the following key elements:

- code of conduct/ethics
- hotline/whistleblower program
- hiring and promotion (i.e., background checks)
- investigation and remediation of identified fraud
- oversight by the audit committee and board
- risk assessment

Management should consider each of these elements in its documentation and evaluation of its anti-fraud program. Additionally, management's documentation should adequately support its assessment of anti-fraud programs and controls by

- providing sufficient information regarding the flow of transactions, which enables management to determine where material misstatements could occur as a result of fraud
- determining which controls prevent and detect fraud
- determining (1) who will perform the controls and (2) the related segregation of duties

Audit Committee Effectiveness

The company's board of directors is responsible for evaluating the performance and effectiveness of the audit committee and demonstrating its assessment to the external auditors. When evaluating the effectiveness of the audit committee, we believe the board should consider the following:

- independence of the audit committee from members of management
- clarity with which the audit committee's responsibilities are articulated and how well the audit committee and management understand those responsibilities

- level of involvement and interaction with the external auditor, including the committee's role in the appointment, retention, and compensation of the external auditor
- level of involvement and interaction with internal audit, including the committee's authority and role in appointing and compensating employees in the internal audit function
- interaction with key members of financial management, including the chief financial officer and chief accounting officer
- extent of questions raised by the audit committee and its responsiveness to concerns raised by the external auditors
- the audit committee's compliance with exchange listing standards
- the level of financial expertise among the audit committee members
- any ongoing training for audit committee members on accounting and/or industry specific matters

Risk Assessment

Another component of internal control is risk assessment. For an entity to exercise effective control, it must establish objectives and understand the risks it faces in achieving those objectives. As part of its risk assessment process, management should determine and consider the implications of relevant risks that could hinder the achievement of its objectives. Management must then provide a basis for managing the risks. For purposes of management's Section 404 assessment, the Standard indicates that management should identify the risks of material misstatement in the significant accounts and disclosures and related assertions of the financial statements. Management should implement controls to prevent or detect errors or fraud that could result in material misstatements. An example provided in the Standard is that management should assess how it considers the possibility of unrecorded transactions or identifies and analyzes significant estimates recorded in the financial statements.

The process of identifying and analyzing risks is an ongoing iterative process. The sub-components for the risk assessment include:

- Business Risk Assessment
  - Entity-wide objectives – Does the entity have approved entity-wide objectives that are aligned with the strategic plan?
  - Activity-level objectives – Are activity-level objectives consistent with entity-wide objectives and are they relevant?
  - Risk analysis – Are there mechanisms to identify risks and to prevent the entity from achieving its objectives from both internal and external sources? Is the process thorough and relevant?
  - Mechanisms for change – Are there adequate mechanisms to identify change for routine events and for events that may have a pervasive impact on the entity?
- Inherent Risks
- Fraud Risks

Management may address risk in a combination of the following ways:

- Having the internal audit department perform annual risk assessments
- Having business units perform risk assessments in a self-assessment format, which are then consolidated for review by a senior executive who is responsible for risk management or compliance with Section 404
- Making a senior executive responsible for performing independent risk assessments
- Creating a risk council that is charged with overseeing risk assessment
- Having the internal audit department lead the assessment of fraud risk
- Holding weekly/monthly meetings of executive management to discuss key business risks

Control Activities

Control activities are the policies and procedures that help to ensure that management's directives are implemented. Control activities occur throughout the organization, at all levels, and in all functions. The activities involve approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties.

COSO discusses many different types of control activities, including preventive controls, detective controls, manual controls, computer controls, and management controls. Control activities address specified information processing objectives/CAVR, such as ensuring completeness and accuracy of data processing. The following list includes certain control activities that are commonly performed by personnel at various levels in organizations, as indicated by COSO.

- *Top Level Reviews* – Reviews are made of actual performance versus budgets, forecasts, prior periods, and competitors. Major initiatives are tracked (such as marketing efforts, improved production processes, and cost containment or reduction programs) to measure the extent to which targets are being reached. Implementation of plans is monitored for new product development, joint ventures, or financing. Management actions taken to analyze and follow-up on such reporting represent control activities.
- *Direct Functional or Activity Management* – Managers review performance reports to monitor the performance of their department or area of responsibility.
- *Information Processing* – A variety of controls are performed to check accuracy, completeness, and authorization of transactions. Data entered into computer applications is subject to edit checks or matching to approved control files. A customer's order, for example, is accepted only upon reference to an approved customer file and credit limit. Numerical sequences of transactions are accounted for. File totals are compared and reconciled with prior balances and with control accounts. Exceptions are investigated and reported to supervisors as necessary. Development of new systems and changes to existing systems are controlled, as is access to data, files, and programs.
- *Safeguarding of Assets/Physical Controls* – Equipment, inventories, securities, cash, and other assets are secured physically, and periodically counted and compared with amounts shown on control records. These control activities will also contribute to management's antifraud program.

- *Performance Indicators* – Performance indicators include, for example, purchase price variances, the percentage of orders that are "rush orders", and the percentage of returns to total orders. By investigating unexpected results or unusual trends, management may identify circumstances where the underlying procurement activity objectives are in danger of not being achieved. Whether managers use this information only to make operating decisions, or also follow up on unexpected results reported by financial reporting systems, determines whether analysis of performance indicators serves operational purposes alone or financial reporting control purposes, as well.

- *Segregation of Duties* – Duties are divided, or segregated, among different people to reduce the risk of error or inappropriate actions. For instance, responsibilities for authorizing transactions, recording transactions, and handling the related assets are divided. A manager authorizing credit sales would not be responsible for maintaining accounts receivable records or handling cash receipts (each of which is a basic business sub-process). Similarly, salespersons would not have the ability to modify product price files or commission rates.

These examples are just a very few among a myriad of control procedures performed every day throughout an organization that serve to enforce adherence to established business protocols, and to keep entities on track toward achieving their objectives.

Information and Communication

The information and communication component includes the systems that support the identification, capture, and exchange of information in a form and time frame that enable personnel to carry out their responsibilities and financial reports to be generated accurately. Information and communication also spans all of the other components of internal control. When evaluating this component, management must consider internally generated and externally generated data that enable management to make informed business decisions about financial reports and disclosures. Examples of relevant external information include industry, economic, and regulatory information. Communicating relevant data throughout all levels of the company and to the appropriate external parties is an important part of internal control.

Management should focus on understanding the systems and processes that are important in the accumulation of financial data, including the system of controls that safeguard information, the processes for authorizing transactions, and the system for maintaining records. When evaluating the information and communication component of a company's internal control over financial reporting, management should consider the methods that the company uses to accumulate and disseminate information, including

- accounting systems
- policy manuals (including financial reporting manuals)
- management's reports
- newsletters
- accounting policy updates
- technical updates
- staff meetings
- training

When evaluating information and communication, management must consider quality, for example, ascertaining whether:

- Content is appropriate – Is the needed information available?
- Information is timely – Is it available when required?
- Information is current – Is it the latest available?
- Information is accurate – Is the data correct?
- Information is accessible – Can the data be obtained easily by appropriate parties?

All of these questions should be addressed by the system design. If not, it is probable that the system will not provide the information that management and other personnel require to ensure accurate financial reporting.

Monitoring

Monitoring is the continuous processes that management uses to assess the quality of internal control performance over time. There are three sub-components to monitoring:

Monitoring Sub-components	
Ongoing Monitoring	Ongoing monitoring occurs in the ordinary course of operations. Ongoing monitoring includes regular management and supervisory activities and other actions personnel take in performing duties that assess the quality of the internal control system's performance.
Separate Evaluations/ Periodic Monitoring	Periodic monitoring involves less frequent (i.e., monthly or quarterly) activities by senior management. Periodic monitoring occurs when management reviews the internal control system from time to time, focusing directly on system effectiveness. The scope and frequency of separate evaluations will depend primarily on an assessment of risks and ongoing monitoring procedures.
Reporting Deficiencies	The monitoring component should also include a process for reporting deficiencies to the appropriate level of management and the board of directors and undertaking remediation efforts.

Examples of monitoring controls:

- internal audits
- management reviews
- audit committee activities
- disclosure committee activities
- self-assessment reviews

Other Considerations

The period-end reporting process, general computer controls, and company-level controls are not separate components of internal control, however they are important elements of a company's internal control over financial reporting and thus, are discussed separately below.

Period-End Reporting Process

The period-end financial reporting process is always a significant business process because of its importance to financial reporting and the financial statements. Evaluating the design and effectiveness of controls for the period-end financial reporting process is an important step in the overall assessment of internal control over financial reporting.

The period-end financial reporting process includes…	Management should evaluate…
The procedures used to enter transaction totals into the general ledger. The procedures used to initiate, authorize, record, and process journal entries in the general ledger. Other procedures used to record recurring and nonrecurring adjustments to the annual and quarterly financial statements, such as consolidating adjustments, report combinations, and classifications. Procedures for drafting annual and quarterly financial statements and related disclosures.	The automated and manual inputs, procedures performed, and outputs of the processes the company uses to produce its annual and quarterly financial statements. The extent of information technology involvement in each period-end financial reporting process element. Who participates from management. The number of locations involved. The types of adjusting entries. The nature and extent of the oversight of the process by appropriate parties, including management, the board of directors, and the audit committee. The controls over the consolidation process. The method for establishing and monitoring the selection and consistent application of accounting policies. The use of manual spreadsheets and manually compiled data in the consolidation process.

Management is responsible for the controls over the period-end reporting process. The external auditors should not participate in the execution of these controls or be considered a part of management's control over the period-end reporting process. Management must have the expertise (1) to select and apply accounting policies and (2) to form a view over accounting and reporting matters. Management should be able to demonstrate how it develops, approves, communicates, implements, and monitors accounting policies.

The period-end reporting process often involves multiple levels of an organization. Thus it is likely that evaluating and testing the period-end reporting process will extend beyond the parent or corporate level. For example, the following items (if applicable) should be included in the evaluation of the period-end reporting process:

- Manual journal entries that are posted during the process of consolidating the company at the corporate level (e.g., consolidation entries, elimination entries, or other "top level" adjustments)
- Manual journal entries that are posted during a regional consolidation of individual locations that is then submitted to corporate/the parent company for inclusion in the company-wide consolidation
- Manual journal entries posted directly to the general ledger before consolidation at a regional or corporate level (i.e., as part of the reconciliation of a sub-ledger with the general ledger)
- Systematic and transactional postings to the general ledger throughout the course of business (i.e., posting of sub-ledger account balances to the general ledger)

FAQ: How can management enhance its internal control over the selection and application of appropriate accounting policies?

Selecting and applying accounting policies that are consistently communicated and implemented across a company's locations and business units is an important control activity in the period-end reporting process. Management should consider the following control activities in its period-end reporting process as it relates to the selection and application of appropriate accounting policies

- *Monitor activities of the standard-setting bodies through*
  - *newsletters, databases, and websites*
  - *participation in industry and professional committees and conferences*
- *Develop procedures to communicate new accounting policies throughout the company*
- *Ensure policies are established for higher risk (i.e., significant, complex, judgmental) accounts or transactions*
- *Develop and document accounting policies*
- *Employ appropriately skilled individuals*
- *Provide training for individuals responsible for applying policies*
- *Require audit committee approval of critical accounting policies*

Disclosures

Disclosures are an important component of financial reporting. When assessing controls over footnote disclosures, management should ask the following:

- Who is responsible for compiling/computing each of the disclosures in the quarterly and annual reports
- What process is in place to ensure that disclosures meet the requirements of GAAP, the SEC, and other regulatory bodies/standards
- What are the sources of information that support the disclosure process

- How do the individuals who are responsible for the disclosures ensure that the source information is accurate, valid, and complete
- Who reviews the disclosures upon completion
- What are the inputs, procedures, and outputs that are used to produce the financial statements and disclosures
- How have the company's disclosure and audit committees reviewed the control over the financial reporting and disclosure process to ensure all information is properly disclosed
- How does management ensure that subsequent events are identified for disclosure
- How is the segregation of duties addressed within the period-end reporting process
- If spreadsheets are used to summarize financial data for disclosure purposes, what controls cover the input and formulas in the spreadsheet

Timing Considerations

Although many of the period-end reporting controls are applied after year-end (i.e., as the year-end financial statements are being prepared), those controls are relevant to the company's internal control over financial reporting at the reporting date and thus must be considered.

Lessons Learned – Timing of Year-end Procedures

Management should consider reviewing its year-end processes and procedures before year-end to ensure that they are designed effectively. If deficiencies are detected during year-end testing of these "annual" controls, management will unlikely be able to remediate until the following year.

Additionally, management should consider the timing of testing of quarterly financial reporting processes to ensure that sufficient time is allowed for any necessary remediation efforts.

Accounting Estimates and Judgments

Control over accounting estimates and judgments is an important part of internal control over financial reporting. Weak controls in this area could negate an otherwise strong system of internal control. Accounting estimates and judgments often pertain to areas, such as:

- Tax accounts
- Pension liabilities
- Legal accruals
- Environmental accruals
- Restructuring charges
- Impairment analysis and charges
- Hedging effectiveness analysis and entries

When assessing controls for such estimates and judgments, management should understand

- which accounts, estimates, and judgments are manually adjusted at the end of a period
- who prepares the journal entries, estimates, and judgments
- who reviews the journal entries, as well as the assumptions surrounding the estimates and judgments
- what supporting documentation is maintained on file to support the entries
- whether the procedures during the year are different than at year-end

General Computer Controls

Another important aspect of internal control is general computer controls. General computer controls are used to manage and control a company's information technology activities. General computer controls are pervasive controls. The degree to which a company can rely on the integrity of information processing and the effectiveness of automated controls and automated accounting procedures (i.e., calculations and automated postings to accounts) depends on the effectiveness of the general computer controls. Underlying the locations and the processes/cycles are the computer systems, applications, and data centers that facilitate information processing throughout the organization. The processing of information by systems is a key aspect of the information and communication component of internal control. In most companies, the integrity of the financial statements greatly depends on the completeness, accuracy, and timeliness of the information flowing through the company's systems. Also, automated controls over the financial statement assertions are directly dependent on the proper functioning of the underlying applications and their supporting information technology infrastructure.

The general computer control scoping decisions will vary based upon how a company's information technology is organized and managed. Management must identify the systems and applications that have an impact on the financial statements. Management must understand how financial information is generated and map the financial statements and business processes/cycles to the computer systems and applications that enable the initiation, authorizing, recording, and processing of the information. This mapping can then be used to identify the information technology infrastructure (data centers and information technology environments) that support these applications. Only those general computer controls that support processes and applications that, in turn, support significant financial statements accounts and disclosures, need to be documented and tested.

Information processing must not only be considered at the application level, but also at the database, operating system, internal network, and perimeter network levels. For each of these levels, management must consider the controls around five general computer control domains of (1) information technology control environment, (2) program development, (3) program change, (4) access to programs and data, and (5) computer operations (as discussed in the Definition of Key Terms at the end of this document).

Lessons Learned – Assessing General Computer Control Coverage

Some companies (generally those with a centralized information technology function) have not directly linked the business processes/cycles to the supporting applications and information technology infrastructure. For simplicity, companies have included entire data centers within the scope of their Section 404 project. This broad scoping may provide a starting point, but does run the risk of obtaining more coverage than necessary. Also, without directly mapping applications to the business processes/cycles that are in the scope of the project, management may inadvertently exclude certain applications or parts of the information technology infrastructure that are not contained in the main data center(s). Management must be able to demonstrate that necessary coverage over the information technology function has been addressed through its procedures.

Lessons Learned – Information Technology Security Accountability

Information technology security, which comprises the controls governing access to the company's computer systems, is important to safeguarding the company's assets, as well as to maintaining integrity of the company's financial reporting. These controls ensure that only the appropriate people can access and change key financial data. Without adequate information technology security, the integrity of the financial data may be compromised. Information security consists of (1) perimeter security, which protects a company's network and computers and (2) application-level security, which limits to the appropriate parties access to transactions and other data within a computer application, as well as enforces segregation of duties. The assessment of perimeter security should be the responsibility of the information technology organization. Because application-level security is tied to the company's process controls more closely than other components of information technology security, responsibility for documenting and assessing application-level security should rest with the individuals (or teams) responsible for the related business process.

Management should also consider security access to spreadsheets that are held on shared servers.

Company-Level Controls

Company-level controls are one mechanism for management to gain assurance that appropriate controls are operating throughout the company. As discussed previously in this section, management will generally gain assurance over locations that are significant only when aggregated with other locations by evaluating, documenting, and testing company-level controls and possibly through other evidence (e.g., self-assessments, internal audit reviews, and monitoring controls) at these locations. Thus, the assessment of company-level controls is an important element of the Section 404 project. As a practical consideration, management may opt to test and evaluate the design effectiveness of company-level controls first because the results of this evaluation will impact the nature, extent, and timing of additional procedures that may be necessary at these locations. See page 24 for factors that should be considered in deciding at which locations to perform testing.

For companies with numerous locations, it is essential that company-level controls operate effectively. When such controls do not exist or are ineffective, improving company-level controls should be a top priority. Many deficiencies in company-level controls may also require several months to remediate. Inadequate company-level controls may be an indicator that the control environment is ineffective.

Company-level controls should also be considered at individually important locations. Management's evaluation of company-level controls will impact the nature, timing, and extent of tests of controls at individually important locations.

Management should consider where in the organization the company-level controls operate (i.e., corporate level, segment level, business unit level, or a lower level). Although corporate may be responsible for compiling and issuing an accounting policies and procedures manual, management must perform testing at the individual locations to ensure that the policies are being appropriately applied. Company-level controls span the components of internal control and the company's anti-fraud program, which are illustrated in the following table:

Examples of Company-Level Controls*

Components of Internal Control and Anti-Fraud Programs	Human Resources	Enterprise Risk Management	Audit Committee	Internal Audit	Whistleblower	Code of Conduct	Information Technology Environment & Organization	Self-Assessment	Shared-Services	Disclosure Committee	Oversight Other Than Audit Committee (Board, Senior Management)	Policies and Procedures Manual	Period-End Reporting	Business Performance Reviews
Anti-Fraud Program	X	X	X	X	X	X					X		X	
Control Environment	X		X		X	X	X				X	X		
Risk Assessment	X	X	X	X	X			X		X	X			
Control Activities									X				X	X
Information & Communication	X	X	X	X	X	X	X		X	X	X	X	X	
Monitoring			X	X	X			X		X	X	X		

*The “X’s” represent areas within the five components of internal control and a company’s anti-fraud program where company-level controls are evidenced.

SECTION IV: Use of Service Organizations

Many companies use outside service organizations to process financial data. Management is ultimately responsible for the internal control over this financial information and therefore may need to assess the design and operating effectiveness of the service organization's internal control, including all five components of internal control. This responsibility is consistent with management's obligations under Section 404 to assess the design and operating effectiveness of internal control over financial reporting.

Lessons Learned – Developing an Inventory of Service Organizations

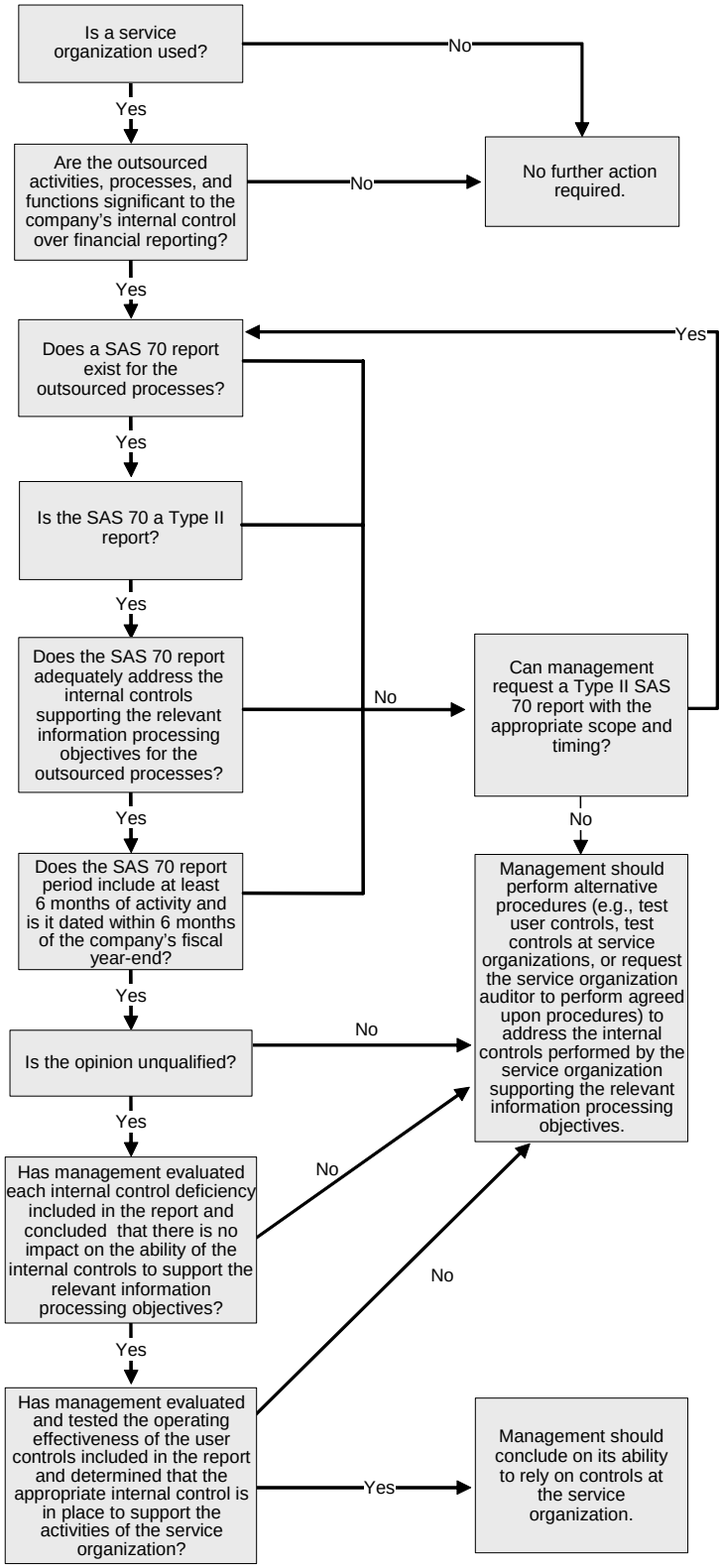
In a large company, developing and managing the list of outsourced operations can be challenging. Management should create a summary of its service organizations, detailing key information about the company's outsourcing arrangement with each service organization (i.e., summarizing the services provided, indicating whether the company is allowed to audit the service organization, determining whether a SAS 70 report exists, and noting the expiration date of the contract) and track the results of and rationale for decisions, based on the decision tree below. To develop an accurate summary, a company should start with the list of vendor contracts that are typically maintained by the company's supplier and legal departments. It is likely that management will identify additional service organizations in the scoping and documentation phases of the Section 404 project. Management will need to determine which procedures to apply to each outsourcing arrangement to comply with the requirements of Section 404.

Management should consider the following steps when evaluating the procedures to perform over its service organizations:

1. Determine if a service organization is being used.
2. Determine if the outsourced activities, processes, and functions are significant to the company's internal control over financial reporting.
3. Determine if a Type II SAS 70 (SAS 70), *Service Organizations* (defined on page 41), report exists and is sufficient in scope.
4. If a Type II SAS 70 report does not exist, determine alternative procedures.

This process is summarized in the decision tree below and explained further in the remainder of this section.

SAS 70 Decision Tree



The Steps for Evaluating the Procedures to Perform Over Service Organizations

Determine If a Service Organization Is Being Used

Many companies outsource activities to service organizations. However, not all outsourced situations will be within the scope of a Section 404 assessment. Generally, an outsourcing situation would need to be considered for a Section 404 assessment only when the outsourced activities constitute a significant process or function performed by a third party that generates information significant to the financial reporting process.

When identifying service organizations, management should distinguish between service organizations and specialists. For example, management may use a specialist to perform:

- valuations (e.g., special purpose inventories, high technology materials or equipment, or complex financial instruments)
- determinations of physical characteristics relating to quantity on hand or condition (e.g., quantity or condition of minerals, mineral reserves, or materials stored in stockpiles)
- determinations of amounts derived by using specialized techniques or methods (e.g., actuarial determinations for employee benefit obligations and disclosures)
- interpretations of technical requirements, regulations, or agreements (e.g., potential significance of contracts or other legal documents or legal title to property)

These specialists are not part of an outsourced process and would not need to be evaluated as if they were part of a company's internal control over financial reporting. However, the output of a specialist's work is often significant to the financial statements. Thus, management should have controls in place (such as a means to evaluate the specialist's professional qualifications) to assess whether the specialist has the required skills and knowledge in the particular field to make an appropriate determination. Similar to Auditing Standard Section No. 336, *Using the Work of a Specialist*, management should also understand:

- The objectives and scope of the specialist's work
- The methods or assumptions used
- How the methods or assumptions used compare to those used in the preceding period

Determine If the Outsourced Activities, Processes, and Functions Are Significant to the Company's Internal Control over Financial Reporting

Management need consider only outsourced operations that are part of business processes management deems significant to its internal control over financial reporting. Auditing Standard Section No. 324, *Service Organizations* (SAS 70 or AU 324), indicates that activities are considered part of a company's internal control if they affect any of the following:

- the classes of transactions that are significant to the company's financial statements
- the procedures, both automated and manual, by which the company's transactions are initiated, recorded, processed, and reported from their occurrence to their inclusion in the financial statements

- the related accounting records, whether electronic or manual, supporting information, and specific accounts in the company's financial statements involved in initiating, recording, processing, and reporting the company's transactions
- how the company's information system captures other events and conditions that are significant to the financial statements
- the financial reporting process used to prepare the company's financial statements, including significant accounting estimates and disclosures

When addressing whether a particular service organization affects a company's internal control over financial reporting, management should consider the significance of the financial statement assertions and the information processing objectives/CAVR for the process being outsourced. If the controls covering one or more information processing objectives/CAVR or financial statement assertions reside principally at the service organization, it is likely that the service organization affects the financial reporting process and will need to be evaluated.

If the activities being performed at the service organization are considered part of the company's internal control over financial reporting, management must determine the extent of procedures, which may include:

- Obtaining a Type II SAS 70 service auditor's report and evaluating the user organization's controls over the activities of the service organization (including those user controls listed in the SAS 70 report)
- Performing tests of controls at the service organization
- Obtaining a report on the application of agreed upon procedures that describes the tests of relevant controls
- Performing tests of the user organization's controls

Depending on the significance and risk of the outsourced process, a combination of these options may be required.

Determine If a Type II SAS 70 Report Exists and Is Sufficient in Scope

SAS 70 provides for a service organization (such as a payroll-processing company) to obtain a single audit report for use by its clients' auditors to plan and conduct audits of financial statements. One of the objectives of SAS 70 was to preclude the need for each user auditor to conduct its own audit of the service organization's controls.

If management determines that the controls at the service organization must be assessed, management should determine if a Type II SAS 70 report exists. If so, management should evaluate whether the report adequately addresses the information processing objectives/CAVR relevant to the company's needs. If a Type II SAS 70 report does not exist or the report is not adequate to meet management's needs, an adequate report should be requested or alternative procedures should be performed. When evaluating a SAS 70 report for its adequacy for reliance, management should consider the following:

Type I or Type II report – A Type I report covers only the suitability of the controls' **design**, whereas a Type II report also assesses whether the controls are **operating effectively** (i.e., the controls are tested by the service organization's auditor). Because the Standard requires management to assess the design **and** operating

effectiveness of its internal control over financial reporting, a Type I report cannot be used for management's Section 404 assessment to support operating effectiveness.

Scope of the audit – The report must cover the processes and controls relevant to management's assessment process. To ensure that this objective is met, management should collaborate with its service organization to determine the scope of the SAS 70 report. A SAS 70 report should cover (1) the relevant information processing objectives/CAVR that are addressed at the service organization and (2) the general computer controls for any applications relevant to management's assessment process.

Some service organizations have multiple processing sites. Management must ensure that the processing location responsible for providing its services is covered by the report. If not, additional procedures will be required.

User controls – In most situations, to conclude that effective internal control over financial reporting exists, management must demonstrate effective controls at both the company and the service organization. The company's controls over the service organization are referred to as "user controls" and are typically documented in the SAS 70 report. Management should evaluate and test these controls. For example, the integrity of outsourced payroll processing will depend on the integrity of the inputs from the company, including information relating to new employee, terminations, and salary increases. If the company is responsible for providing this information to the service organization, the user controls vis-à-vis this information will be important to ensure the overall integrity of the payroll-processing output from the service organization.

Period of time covered – Management must consider the period of time covered by the Type II SAS 70 report. Although the PCAOB staff's FAQs (refer to Question 25 in Appendix IX) do not establish any "bright lines" as it relates to the elapsed time between the date of the SAS 70 report and the date of management's assessment, we believe that a report as of a date earlier than six months prior to the company's fiscal year-end date would result in limited benefits because of the extent of additional procedures that would be necessary. However, if a report's date is too close to year-end, management may be unable to obtain the report in sufficient time to allow for evaluation and remediation.

As the intervening period between the date of the SAS 70 report and the year-end of the company increases, management should consider update procedures. Management should consider whether, during the intervening period, there have been any:

- changes in personnel with whom management interacts at the service organization
- changes in reports or other data received from the service organization
- changes in contracts or service level agreements with the service organization
- errors in the service organization's processing

Based upon these considerations and the significance of the services to the company, management should determine the extent of any further procedures.

Opinion – Management should determine if the service auditor's opinion is unqualified (i.e., in the auditor's opinion, the service organization's controls are designed effectively and are operating as designed). If the opinion is qualified, management should assess the nature of the internal control deficiencies and their impact on the company's internal control over financial reporting. In this case, management may need to perform additional procedures in order to obtain assurance over the service organization's controls or request that the service organization remediate the internal control deficiencies prior to its fiscal year-end.

Additionally, the SEC staff has indicated in its FAQs (refer to Question 14 in Appendix VIII) that management would be able to rely on a SAS 70 report that is issued by its external auditor, as long as management did not engage its external auditors to perform the SAS 70 audit at the service organization.

Testing Exceptions – Although the service auditor may have issued an unqualified opinion, exceptions in testing may exist. Management should evaluate the implications of these exceptions in the area that is being tested (nature, extent, and risk) as it would if exceptions to an internal process were identified.

Additional Procedures – We believe that in some cases, a Type II SAS 70 report will not be sufficient for management's assessment of internal control over financial reporting. For example, if a company outsources substantially all general-ledger and transaction-processing functions to a service organization, the company may conclude that a Type II SAS 70 report would not provide sufficient evidence of operating effectiveness due to the significance of the outsourced processes. In this situation, management should assess whether additional procedures need to be performed to evaluate the design and operating effectiveness of the service organization's controls. Conversely, if a service organization performs routine payroll processing for many customers, it is likely that the service organization's clients would conclude that a Type II SAS 70 report sufficiently assesses the design and operating effectiveness of the service organization's controls.

Lesson Learned – Service Organization Timing

Obtaining a Type II SAS 70 report from a service organization for the first time can be a lengthy process. The service organization may need to remediate certain processes, and thus it often takes six months to a year to obtain a final report after a request is made. Accordingly, companies using service organizations should make this determination as soon as possible.

If a Type II SAS 70 Report Does Not Exist, Determine Alternative Procedures

If a Type II SAS 70 report cannot be obtained, or the report obtained does not adequately address the information processing objectives/CAVR required by management, alternative procedures should be performed over the service organization's internal control. These procedures may include one or more of the following:

- Perform tests of controls at the service organization
- Obtain a report on the application of agreed upon procedures that describes the tests of relevant controls
- Perform tests of the user controls over the activities of the service organization

Perform tests of controls at the service organization

If the company's contract with the service organization has a "right to audit" clause or the company is otherwise permitted by the service organization to perform an audit, management may have its own personnel (typically the internal audit department) review and test the controls at the service organization. This review would be similar to the assessment that management would perform on its internal processes. The review would need to cover the control activities at the service organization, as well as any relevant controls covering the other four components of internal control (including general computer controls).

Obtain a report on the application of agreed upon procedures that describes the tests of relevant controls

The Standard indicates that an agreed upon procedures report may be used if it provides a level of evidence similar to a SAS 70 report. If an agreed upon procedures report is to be relied upon for Section 404 purposes, management should consider the following factors:

- the service organization's controls that (1) are relevant to the company's internal control over financial reporting and (2) cover all five components of internal control (including general computer controls).
- the time period covered and the nature and results of the tests that the service auditor applied to the service organization's controls to validate that they are operating effectively.

Perform tests of the user controls over the activities of the service organization

Management should assess whether its user controls would provide adequate assurance by considering whether (1) a breakdown of control at the service organization could lead to a misstatement that is more than inconsequential and (2) management's user controls would detect or prevent the misstatement in a timely manner.

For example, assume that a company uses a service organization for trust accounting. The service organization updates the company's securities on a monthly basis to reflect current pricing information. On one occasion, the service organization erroneously updates the securities with last month's pricing information, causing the securities to be valued incorrectly. If management performs an independent price comparison on a monthly basis, the error would be detected in the reconciliation, researched, and resolved before the error was recorded in the company's financial records. In this case, management may be able to rely on its own user controls.

User controls may take the form of:

Input/Output Controls — In most outsourcing situations, the company will have some access to the information processed by a service organization. In some cases, this information may enable the company to fully reconcile the service organization's results with the results of an independent source. For example, a company using a payroll service organization could compare the data submitted to the service organization with reports or information received from the service organization after the data has been processed. The company also could recompute a sample of the payroll amounts for clerical accuracy and review the total amount of the payroll for reasonableness.

Performance Monitoring — Management may have a process for monitoring the service organization's performance in relation to various metrics, as typically defined in a service level agreement. Most of these metrics will be tailored to specific operations; in some situations, however, such monitoring may provide some indirect assurance that the service organization's controls are operating properly. For example, management may regularly review the security, availability, and processing integrity of service level agreements and related contracts with third-party service organizations. A designated individual would be responsible for regularly monitoring the third party's performance and reporting whether that performance meets certain criteria.

Process Controls — In some outsourcing situations, the company's user controls may be closely tied to the service organization's processes and provide direct assurance over their operation. For example, a company that has outsourced its information technology development to a service organization may choose to document, track, approve, and test all application changes internally, thus retaining significant control over the information technology development process.

Typically, management's testing of its user controls that pertain to a service organization is not as effective as management's testing of controls that are in place at the service organization itself. Accordingly, management should determine whether an assessment of the company's user controls alone is sufficient to establish the reliability of the relevant information processing objectives/CAVR. We believe management may rely solely on testing its own user controls in situations where (1) such controls cover all relevant assertions over the accounts and disclosures effected by the outsourced processes and (2) the significance and risk of processing at the service organization to the overall user organization's financial statements is low.

FAQ: For international operations, can management rely on reports developed under international standards?

Conceptually, management could rely on reports issued under other standards if those reports meet the criteria under the Standard and SAS 70, as summarized above. For example, we believe that the need for a third-party audit report would be met if performed under the Canadian Institute of Chartered Accountants Handbook Section 5900, Opinion on Control Procedures at Service Organizations*, since this standard (1) closely follows the criteria of SAS 70 and (2) uses Guidance on Criteria of Control (CoCo; published by the Canadian Institute of Chartered Accountants), a suitable internal control framework. Management would also need to evaluate the competency and qualifications of the auditor performing the examination. However, not all countries have developed standards that follow the criteria of SAS 70. Accordingly, management should evaluate carefully the qualifications of the auditor performing the examination and the standards being applied by the service organization's auditor.*

FAQ: What factors should be considered by management when a service organization outsources certain functions to another service organization?

A company may use a service organization that, in turn, uses another service organization (a sub-service organization). To assess internal control over financial reporting, management may also need to consider controls at the sub-service organization.

Management should consider the following factors when evaluating a sub-service organization:

- *the nature and materiality of the transactions processed by the sub-service organization*
- *the contribution of the sub-service organization's processes in the achievement of the user organization's information processing objectives*
- *the availability of a sub-service organization's SAS 70 report*

Because a user organization typically does not have any contractual relationship with the sub-service organization, a user organization should obtain available reports and information about the sub-service organization from the service organization.

SECTION V: Documentation – Evidence of Effective Internal Control

The documentation produced in the Section 404 project forms the basis and support for management's evaluation of internal control over financial reporting. Further, the SEC's final rules on Section 404 indicate that it is a company's responsibility to document internal control, and that developing and maintaining such documentation is inherent to effective internal control.

We believe management's documentation should support its:

- Scoping decisions
- Evaluation of whether the company's system of internal control is designed to prevent or detect material misstatements
- Conclusion that the tests of operating effectiveness were appropriately planned and performed
- Consideration of the test results when determining its assertion

We believe that, to meet its responsibility, management should perform four steps in documenting its internal control:

1. **Determine scope of documentation –** Determine which accounts and disclosures will be evaluated and which locations should be included in the scope of the company's internal control documentation.

2. **Develop process documentation –** Document the flow of transactions for significant accounts and disclosures to determine where material misstatements due to error or fraud could occur. Identify the control activities within these processes.

3. **Develop control documentation –** Document controls within each of the five components of internal control and specifically address company-level controls, anti-fraud programs, and evaluation of the audit committee's effectiveness.

4. **Assess the design of controls –** Evaluate whether the company's controls are adequately designed to mitigate the risk of material misstatement.

Depending on its progress in this phase, a company may need to perform the steps concurrently (instead of sequentially) in order to meet the deadline.

Lessons Learned – Documentation Methodology
We have observed that most Section 404 project teams find that breaking down the documentation and evaluation of internal control by significant process is the most effective approach. Management should map processes to significant accounts, financial statement assertions, and individual controls to ensure appropriate coverage.

Step 1: Determine Scope of Documentation

We believe management should document the controls related to significant accounts, disclosures, and processes at the locations/business units that fall within the scope of the project (in-scope processes), as described in Section III, Scoping and Planning - The Beginning of an Effective Project. Such locations and business units include

1. Individually important locations and business units

2. Locations and business units that are not individually important but pose specific risks that make them important

3. Locations and business units that are not individually important but that could be important when aggregated with other locations or business units

In addition, we believe management should have at least a minimum level of documentation of controls at locations/business units that are not considered significant, either individually or in the aggregate.

We believe the aforementioned documentation requirements are consistent with the SEC's requirement to maintain adequate books and records (refer to Question 18 in the SEC staff's FAQs in Appendix VIII).

Step 2: Develop Process Documentation

Management's documentation of processes related to significant accounts and disclosures must cover more than just the controls that management plans to test. Documentation should (1) enable management to understand the processes underlying the significant accounts from beginning to end and (2) cover the initiation, authorization, recording, processing, and reporting of individual transactions. For example, management should document the entire revenue process, from the initial sales transaction to the recording of revenue and accounts receivable in the general ledger. Without such documentation, it would be difficult to identify (1) points in the process where a misstatement due to error or fraud could occur and (2) the controls covering all relevant information processing objectives/CAVR or financial statement assertions.

Documentation of processes might take various forms: flowcharts, policy manuals, accounting manuals, narrative memoranda, decision tables, procedural write-ups, and completed questionnaires. No single particular form of documentation is required, and the extent of documentation may vary depending on the company's size and complexity. We have found, however, that flowcharts, supplemented by narrative descriptions, are frequently the most effective form of process documentation.

See Appendix V for guidelines on flowcharts.

FAQ: If a company already has extensive documentation (flowcharts, narratives, documentation of operating procedures, etc.), does it need to create documentation specific to the requirements of the Act?

A company should leverage its existing documentation when conducting its Section 404 assessment. Often, however, we have found that this documentation (1) is not current, (2) is not presented in a format that facilitates management's assessment, and (3) does not cover all of the information required by the Act.

FAQ: If a company already has extensive documentation (flowcharts, narratives, documentation of operating procedures, etc.), does it need to create documentation specific to the requirements of the Act? *Continued*

Most companies are striving for documentation in similar formats to supply all of the information required by the Act across their locations/business units. Consistent documentation makes it much easier for the company to efficiently evaluate the effectiveness of internal control. However, management needs to weigh the costs and benefits of developing a new comprehensive documentation approach. Some companies may be able to satisfy Section 404's documentation requirements by simply improving their current documentation. Other companies may elect to start with a "clean piece of paper" approach. When evaluating the costs and benefits of either approach, management should consider the long-term benefits of doing the latter. Since the Section 404 assessment is performed annually, savings will accumulate over time.

Step 3: Develop Control Documentation

Once management has documented the in-scope processes, it should document the design of the controls that are relevant to financial reporting. This documentation allows management to assess whether the controls cover the financial statement assertions that were mapped to each account during the scoping phase. Management's documentation of the controls' design should encompass the five internal control components of the COSO framework.

In assessing the design of controls, management determines whether the controls (procedures, processes, policies, and systems) will, if operating as intended, provide reasonable assurance that management's control objectives are being met vis-à-vis the relevant financial statement assertions for all significant accounts and disclosures (often referred to as design effectiveness). Management will evaluate the operating effectiveness of controls during the testing phase of the project. However, if the design of a control is flawed, the company will not achieve the desired assurance that the control is capable of preventing or detecting a misstatement even if the control is operating as intended. Management will need to remedy design deficiencies.

FAQ: At what level of the organization (corporate, business unit, process, etc.) does a company need to document all five components of internal control?

This will vary with the particular component of internal control and how the company manages its business:

- *Control Environment – starts at the corporate level, but companies will need to demonstrate that the control environment operates at all levels of the organization.*
- *Risk Assessment – generally needs to be documented only at the corporate level, unless a particular business unit or department has its own specific risk assessment process that is relevant to financial reporting.*
- *Control Activities – generally take place at all levels (for example, financial reporting control activities take place at a corporate level, various reconciliations and period-end controls take place at the business unit level, and routine processing controls take place at the transaction level).*
- *Information and Communication – encompasses all levels of the organization and tends to be embedded in the other components, particularly in the control activities component.*

FAQ: At what level of the organization (corporate, business unit, process, etc.) does a company need to document all five components of internal control? *Continued*

- *Monitoring – encompasses the following:*
  - *Separate Evaluations – includes less frequent activities by senior management and can generally be documented at the entity level*
  - *Ongoing Monitoring Activities – includes regular management and supervisory activities and can generally be documented with the control activities*
  - *Reporting Deficiencies – includes a process for reporting internal control deficiencies to the appropriate levels of management and board of directors*

The company should document the design of controls that cover

- relevant assertions related to all significant accounts and disclosures in the financial statements (encompassing the five components of internal control, including period-end reporting and company-level controls);
- the prevention and detection of fraud, including who performs the control and the related segregation of duties.

The Standard indicates that a deficiency in relation to the safeguarding of assets (e.g., controls to prevent the theft of inventory) would not constitute a material weakness or significant deficiency if the company had a detective control (e.g., a physical inventory count) that would prevent a material misstatement of the financial statements on a timely basis.

The Standard includes guidance and examples of controls that safeguard assets. We expect that the guidance surrounding safeguarding of assets will continue to be a significant topic of discussion as companies determine which controls to test.

FAQ: What is the recommended form of documenting the design of controls? How deep within the organization must the documentation go? How detailed does the documentation need to be?

Management must carefully consider the extent of documentation that it must provide to demonstrate the design effectiveness of internal control. A level of detail that goes beyond what is necessary will result in excess documentation, which in turn may lead to unnecessary testing of controls. We believe management's documentation of the design of controls should be sufficiently detailed to allow a person who knows little about the process to understand and evaluate whether the controls are designed effectively, enabling that person to create a test plan. A lack of documentation limits the ability of management to properly communicate the control processes throughout the organization and properly monitor internal control.

We believe standard practice for documenting the evaluation of controls is to use a detailed control matrix. While not required, control matrices have been effectively used in practice for many years. Matrices are beneficial in that they

- *Provide a rigorous framework, helping to ensure that all relevant controls are adequately documented*
- *Provide a structured mechanism for identifying control deficiencies*

FAQ: What is the recommended form of documenting the design of controls? How deep within the organization must the documentation go? How detailed does the documentation need to be?
Continued

- *Facilitate the use of standard documentation of controls*
- *Facilitate the auditor's review process*

The control matrices should be linked to the flowchart and/or narrative for easy cross-reference.

Although the control matrix may take many forms, it should break down each process into sub-processes, all of which should address information processing objectives/CAVR and ultimately, the relevant financial statement assertions. Documentation of control activities should, at a minimum, provide answers to the following questions:

1. ***What** is the risk being controlled?*
2. ***What** is the control activity?*
3. ***Why** is the activity performed?*
4. ***Who** (or what system) performs the control activity?*
5. ***When** (how often) is the activity performed?*
6. ***What** mechanism is used to perform the activity (reports and systems)?*

The control matrix should illustrate other key attributes that will enable management to assess the adequacy of the controls and develop test plans. These attributes typically address the nature of the control (manual or automated), whether the control is preventive or detective, the frequency of the control, the financial statement assertion being addressed, and the information processing objective being addressed.

(See Appendix VI for a sample control matrix.)

Lessons Learned – Documentation That Addresses the Identified Risk

*Management's documentation of the company's controls should clearly define the **control** that addresses a risk and not just the **process or activity**. Often this distinction may be confusing. For example, creating a spreadsheet that compares bank deposits to receipts is an activity in the cash reconciliation process. Someone investigating the reasons for any differences and resolving them represents a control that should be evidenced through signature, initials, or other visible means that the control was performed.*

Documentation of General Computer Controls

The following table is an overview of what must be documented for each domain and the linkage to each financial statement assertion.

Domain	What Must be Documented?	Financial Statement Assertions Affected
Information Technology Control Environment	Each information technology organization deemed to be in-scope	All
Program Development	Significant development projects underway	All
Program Changes	All in-scope applications and information technology environments	All
Access to Programs and Data (Security)	All in-scope applications and information technology environments	All – but most relevant to completeness and existence
Computer Operations	All in-scope information technology environments	All – but most relevant to completeness

We believe each of these domains should be documented and assessed using the same basic methodology and tools that are used for other control activities. Thus, a control matrix should be created for each of the five domains indicating the control objectives covering the key sub-components of each domain.

Lessons Learned – Leverage Common Elements of Information Technology

In large information technology organizations, there are generally common processes across information technology organizations supporting different business units or geographies. In these cases, separate control matrices for each application or information technology environment may not be necessary. A common control matrix, documenting the standard process, can be developed. Exceptions to this standard process may then be documented in a matrix specific to an application or environment. For example, some companies have a common program change process across several applications. If this is the case, a generic control matrix covering the standard process can be developed and the control activities documented.

Documentation of All Components of Internal Control

Management should have evidence that controls over all components of internal control exist. Regarding the appropriate level of documentation:

- Documentation should address the sub-components of each component of internal control. The sub-components are discussed in the Definition of Key Terms section of this monograph and Section III: Scoping and Planning – The Beginning of an Effective Project.
- Supporting documentation, such as code-of-conduct documents, self-assessments, and documentation of organizational structures, should exist.
- Documentation should include the results of management's testing and evaluation.

Step 4: Assess the Design of Controls

After management has documented the design of the controls for the in-scope processes, it must determine (1) the effectiveness of the design of controls and (2) which controls must be tested for operating effectiveness. These two steps are closely linked; however, we will present them sequentially for ease of discussion.

Effectiveness of the Design of Controls

The evaluation of design effectiveness addresses whether the system of internal control is suitably designed to prevent or detect on a timely basis, material misstatements in significant accounts and disclosures. This evaluation should cover (1) pervasive company-level controls (management should assess the internal control components of control environment, risk assessment, information and communication, and monitoring) and (2) specific transaction-level control activities related to all relevant assertions for all in-scope processes. When assessing design effectiveness, management should focus on:

- The alignment between the controls and the business and audit risks identified (i.e., whether the business processes and related controls appear to be effective in achieving management's stated objectives and managing its risks)
- Whether the controls satisfy the information processing objectives/CAVR and the relevant financial statement assertions
- Frequency of the control – whether the control will detect or prevent the risk identified on a timely basis (i.e., in some cases, a detective control may be adequate, but in other cases, an entity should ensure adequate preventative controls are in place)
- Knowledge and experience of the people involved in performing the controls
- Segregation of duties relevant to the process being controlled
- Timeliness in addressing issues and exceptions that result from the control activity
- Reliability of the information used in the performance of the control
- Period covered by the control

Not all controls provide the same level of assurance. In evaluating the level of assurance provided by a given control, management should consider the nature of the control, how the control is applied, the consistency with which it is applied, and who applies it. The degree of assurance over internal control will vary based on several factors, including those listed below:

Less Assurance	Greater Assurance
Manual control	Automated control
Complex control (requires many steps, multiple calculations, etc.)	Simple control (single step, single calculations, etc.)
Control is performed by a junior, inexperienced person	Control is performed by an experienced manager
Detective control (detects a potential problem after a transaction is executed)	Preventive control (prevents a problem)

Less Assurance	Greater Assurance
Single control	Multiple, overlapping controls
High-level control (analytics)	Detailed, transaction-level control
Control uses sampling	Control involves checking all items
Control takes place well after the transaction	Control occurs in real time (i.e., as the transaction takes place)

Management's evaluation of design effectiveness is important because only properly designed controls can mitigate risk. Thus, management should document its evaluation in a clear and comprehensive manner.

Controls to Test for Operating Effectiveness

In preparation for the next phase of the Section 404 project, management must determine and document which controls will be tested for operating effectiveness. As indicated previously, this determination will naturally be tied to the assessment of design effectiveness. Once again, this will require considerable judgment, and there is no quantitative formula or prescriptive checklist for management to follow. Management must test controls for all relevant financial statement assertions for all significant accounts and disclosures for all individually important locations and significant specific risks. Although one control may cover a specific assertion, the Standard indicates that a combination of preventive and detective controls is generally most effective.

External Auditor Interaction

Since the determination of which controls are key is so critical to management's internal control assessment, the external auditor should be kept informed of management's decisions as to what controls are key. Some companies are holding regular "key control" meetings with the external auditor to review such decisions.

The controls that are to be tested have been designated "key controls" by some companies. Other companies use a rating scheme (i.e., high/medium/low) to define the degree of assurance a control provides. A company may, for instance, plan to test only the high- and medium- rated controls. No single scheme is necessarily correct. For simplicity, we will refer to controls that will ultimately be tested for operating effectiveness as key controls.

Lessons Learned – Determining Key Controls

Assessing design effectiveness and determining which controls to test should be assigned to experienced people — preferably people with a background in controls assessment or auditing and the process owners. The process owners should be accountable for these decisions.

The table below summarizes examples of items that management should ensure are available to support its assessment.

Examples of Items to be Included in Management's Documentation	
Scoping	■ Identification of significant/individually important locations (including quantitative metrics and specific risks) ■ Identification of significant accounts and disclosures (including materiality) ■ Identification of significant processes and sub-processes ■ Coverage analysis
Process Flow	■ Mapping of significant accounts to processes and relevant assertions ■ Flowcharts or narratives describing processes, sub-processes, and controls over relevant assertions, including the period-end financial reporting process
Control Environment	■ Board minutes ■ Human Resource policies and procedures manuals ■ Job descriptions ■ Employee files ■ Personnel listings ■ Employee turnover statistics ■ Operating reports ■ Organization charts ■ Assessment of Audit Committee effectiveness
Risk Assessment	■ Company objectives and associated risks to achievement ■ Reports submitted to the Board of Directors and/or Audit Committee ■ Risk analyses and assessment ■ Disclosure Committee minutes ■ Fraud risk assessment
Monitoring	■ Internal Audit reports ■ Internal Audit workpapers ■ Self-assessments
Antifraud Programs and Controls	■ Code of Conduct ■ Confirmations of Code of Conduct ■ Reports on hotline complaints ■ Procedures for resolving complaints ■ Logs of reported incidents
Information and Communication	■ Financial reporting procedures manual ■ Accounting policies and procedures ■ Organizational structures indicating the lines of reporting and communication relevant to financial reporting ■ Company policies related to distribution of information
Management's Evaluation of Design	■ Management's conclusion on design effectiveness ■ Identified deficiencies, if any, and impact on evaluation

Examples of Items to be Included in Management's Documentation	
Testing of Operating Effectiveness	■ Testing selections, rationale for selection, and identification of key controls for testing ■ Details of tests ■ Management's conclusion on operating effectiveness ■ Identified exceptions, if any, and impact on evaluation
Evaluating Deficiencies in Internal Control Over Financial Reporting	■ Control deficiencies, significant deficiencies, and material weaknesses from all sources (Internal Audit, external auditor, etc.) ■ Compensating controls ■ Results of aggregation of deficiencies ■ Management's report on its assessment of the effectiveness of internal control over financial reporting

SECTION VI: Testing – Determining the Operating Effectiveness of Internal Control

To demonstrate effective internal control over financial reporting, management should determine whether the company's controls are operating effectively. This requires testing the controls, which must include each of the five components of internal control over all relevant assertions for all significant accounts and disclosures at each individually important location and over the specific risk areas at other locations. The company must retain evidence of this testing to support management's assessment of internal control over financial reporting.

The testing phase of the Section 404 project can be divided into four key steps:

1. Identify the controls to be tested
2. Identify who will perform the testing
3. Develop and execute the test plans (what, how, and when to test)
4. Evaluate the test results

These steps will typically be performed sequentially, but some aspects will be iterative as the results of testing necessitate changes in the plan or the need for retesting of remediated items.

These steps should be described in the company's overall testing strategy; key members of management (i.e., the project's steering committee) should review and approve the test plans, which detail management's philosophy and approach to the testing phase. Testing will require a significant effort. Management should not underestimate the amount of time required and the complexities that will be encountered during the testing phase of the project. One way to ensure that the test strategy is applied consistently across a company is through a company-wide training effort.

External Auditor Interaction

We recommend an open dialogue with the external auditor regarding management's testing strategy. The external auditor also should assess the detailed test plans.

Management's assessment of the effectiveness of internal control over financial reporting is expressed at the level of reasonable assurance. The concept of reasonable assurance is built into the definition of internal control over financial reporting and also is integral to the auditor's opinion. Reasonable assurance includes understanding that there is a remote likelihood that material misstatements will not be prevented or detected on a timely basis. Although not absolute assurance, reasonable assurance is, nevertheless, a high level of assurance.

In order to obtain a high level of assurance, management must obtain sufficient competent evidence about the design and operating effectiveness of controls over all relevant assertions related to all significant accounts and disclosures in the financial statements at each individually important location. While the auditor's evidence of operating effectiveness will generally come from traditional testing (i.e., select a sample and reperform the control), management has more latitude in how it obtains the necessary evidence. For example, management

may be able to obtain evidence of design and operating effectiveness through a self-assessment process, internal audit reviews, or ongoing monitoring activities. This is not to suggest that management can avoid sampling and testing of key controls. Rather, management can use alternative sources of evidence (if available) in combination with detailed sample testing to achieve a high level of assurance. In this regard, management may not detail test every control in the same manner as the auditor. In developing its testing plan, management will need to consider whether it has sources of evidence beyond what it will obtain from detailed sample testing. Where management concludes such evidence exists, it may decide to reduce the sample sizes below what the auditor concludes is necessary to achieve a high level of assurance. In those cases, we generally believe management should use sample sizes that when combined with other tests performed (i.e., self-assessment, etc.) would result in the total number of items tested by management to evaluate the operating effectiveness of a key control to be at least equal to the minimum sample sizes presented in the tables in this section. If management does not have other sources of evidence available, we believe the sample sizes used by management should be more than the minimum sample sizes presented in the tables in this section when an individual control is the sole control related to one or more financial statement assertion for a significant account or disclosure, a control is considered to be more important, or a higher level of assurance is required. Robust testing by management can significantly reduce the risk of a significant deficiency or a material weakness being identified too late for remediation to occur prior to year-end.

Identify the Controls to Be Tested

Management must demonstrate that controls covering all five components of internal control are operating effectively relative to all significant accounts, processes, and locations. The nature of tests of control activities is typically more straightforward than the tests to be performed for the other components of internal control. Evaluating the effectiveness of controls related to the control environment, risk assessment, information and communication, and monitoring components typically requires greater judgment and qualitative analysis than is required for an evaluation of control activities.

The locations selected and the testing performed should follow from the decisions made during the scoping and documentation phases of the project, as reiterated below:

Category	Minimum Account Balance Coverage	Location	Planned Procedures
1	60 – 70%	Individually important locations and Accounts with specific risks	Detailed evaluation and tests of controls over significant (or "specific risk") accounts and disclosures at that location and testing of company-level controls.
2	25 – 35%	Locations considered important when aggregated	Evaluate and test company-level controls, if applicable, and consider obtaining other evidence or perform some tests of controls at locations if company-level controls do not exist.
3	<5%	Immaterial locations, individually and in the aggregate	No testing required.

For category 1 locations, testing would include transaction-level controls over the significant accounts and processes and company-level controls. For category 3 locations, no specific control testing is required. For category 2 locations, if company-level controls are in place, management should document and test them to evaluate whether they are operating effectively. For example, in order to determine whether an accounting manual's policies are implemented (a company-level control), management will have to perform testing at selected individual locations in category 2 to determine whether local personnel have applied the policies in accordance with the accounting manual. Management may also decide to obtain evidence about the operating effectiveness of control activities at these locations through other means, such as self-assessments, internal audit reviews, and monitoring controls.

The following table represents our view on the minimum number of category 2 locations that should be subject to testing of company-level controls.

Number of Locations	Number of Locations to Test Company-Level Controls
Less than 20	2 – 4
20 – 49	4 – 6
50 – 100	6 – 10
100+	10 – 20+

If company-level controls cannot be relied upon for category 2 locations, detail testing of controls over significant accounts and disclosures will need to be performed.

Identify Who Will Perform the Testing

The Standard indicates that management may evaluate the operating effectiveness based on procedures such as testing of controls by internal audit, testing of controls by others under the direction of management, using service organization reports, inspecting evidence of the application of controls, or testing by means of a self-assessment process some of which might occur as part of management's ongoing monitoring process. In all cases, management must take responsibility for the work which involves determining whether (1) the personnel who perform the work have the necessary competence and objectivity and (2) the procedures provide evidence sufficient to support management's assessment.

FAQ: Can management allow the person who performs a control to assess the design and operating effectiveness of that control? If so, can the auditor rely on this self-assessment?

The Standard indicates that management can use a self-assessment process, some of which might occur as part of management's ongoing monitoring activities. Independent verification may be required for management to obtain the necessary level of assurance from the self-assessment process.

However, it is clear in the Standard that when evidence of a control's operating effectiveness is furnished by the person who performs that control, the evidence cannot be used by the external auditor to reduce the extent of his/her testing, since the person testing the control will not be sufficiently objective. Management should recognize that self-assessments, by their vary nature lack a degree of objectivity.

Lessons Learned – Quality Assurance

When management believes more objectivity (i.e., the individual responsible for performing the control is not the individual responsible for testing the control) is needed in testing, a quality assurance (QA) role may be introduced. The logical and typically most objective candidate for the QA role is the internal audit department, which could both review the test plans and assess the test results.

Develop and Execute the Test Plans

To facilitate review and approval by the various interested parties, formal test plans should document the key elements of the test and the results. Test plans should cover all controls that are selected for testing and should specify the following key elements:

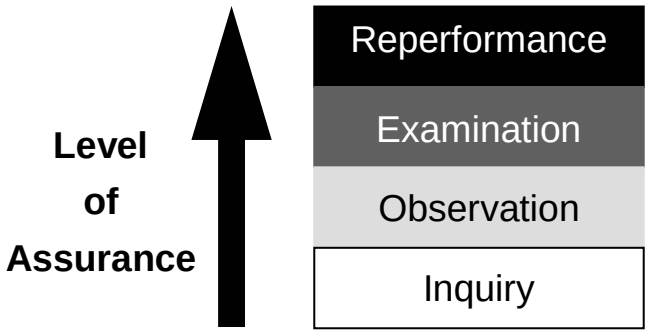
- **Key controls to be tested –** Normally management will summarize the controls to be tested at the financial statement assertion level.
- **Nature of tests to be used –** Tests should be categorized as inquiry, observation, examination, or reperformance.
- **Extent of testing –** The plans should specify the number of items that are to be tested and the method and reasons for selecting those items.
- **Timing of procedures –** The plans should specify when the testing should be performed and the time span that the tests cover, including update testing planned from the interim testing date to year-end.
- **Description of the test –** The plans should specify the procedures to be performed and the assertions supported.
- **Key administrative items –** The plans should identify who will perform the test, when the test will be performed, what evidence will be reviewed, and where the control is performed.
- **Documentation –** The plans should describe the documentation required.
- **Exceptions –** The plans should describe how exceptions will be investigated and addressed and when additional testing should be performed.

Lessons Learned – Structure of Testing Plans

In many cases, a number of controls can be tested with a single sample of transactions that follows the financial process through a sequence of activities, which provides the tester an enhanced understanding of how various controls interact. For example, one technique for testing the controls in a revenue process is to select a sample of new sales contracts. Authorization can be tested by validating the appropriate signatures on the contract. Accuracy of the prices can be verified by assessing whether modified prices (a) match what is specified in the policy and (b) were authorized.

Nature of Tests

The nature of tests can be classified into four categories: inquiry, observation, examination, and reperformance. Combining two or more of these tests can provide greater assurance than using only one technique. The more significant the account, disclosure, or business process and the more significant the risk, the more important it is to ensure that the evidence extends beyond one testing technique. The nature of the control also influences the nature of the tests of controls that should be performed. The relative level of assurance by nature of test is illustrated in the following chart:



Inquiry of a control's effectiveness does not, by itself, provide sufficient evidence of whether a control is operating effectively. **Observation** of the control provides a higher degree of assurance and may be an acceptable technique for assessing automated controls. **Examination** of evidence often is used to determine whether manual controls (e.g., the follow-up of exception reports) are being performed. **Reperformance** of the specific application of the control provides the highest degree of assurance. Most manual controls will be tested through a combination of inquiry, observation, examination or reperformance.

Extent of Testing

The extent of testing of a particular control will vary depending on a variety of factors, including whether a control is automated or manual. Appendix B of the Standard presents examples of the extent of testing decisions that may be useful to management in deciding on a testing approach.

Testing of Automated Controls

For an automated control, the number of items tested can be minimal (one to a few items), assuming that information technology general computer controls have been tested and found to be effective. A common automated control is an edit check that is activated during data entry. Drawing on a database of permissible combinations of services and prices, the edit-check function is designed to prevent the order entry clerk from entering an invalid price for a service. Each attribute of the automated control should be tested for operating effectiveness. In this example, a few different invalid prices/service combinations should be entered to demonstrate that the control is working effectively. In some cases, management override procedures may allow an automated control to be circumvented. This override capability should be evaluated to assess potential internal control deficiencies.

When testing automated controls, management must (1) ensure general computer controls are effective and (2) have performed a detailed review of the controls within the company's computer applications (e.g., a pre-implementation or a post-implementation review). In the previous example, management should have developed a baseline understanding that the edit-check control is designed to work under all circumstances.

If management has never performed a detailed pre- or post-implementation review of the controls for the company's computer applications or there are weak program change controls, it is the responsibility of management to ensure that the automated controls are working as designed. There are several ways to accomplish this objective, from the extreme of program code review to detailed walkthroughs ensuring all relevant logic paths are covered. For third-party software that has not been modified, management should validate that the standard configurations are appropriately set and ensure there is a control process over changes to those configurations. For custom-developed or in-house applications, more extensive procedures to validate the design of the control may be required.

Lessons Learned – Differentiating Between Manual and Automated Controls

In most cases, it will be clear whether a control is manual or automated. However, to novice testers this distinction can be confusing. A control may rely on an automated process, but the key component of the control is manual. For example, a common control includes a systematic three-way match of receiving reports, purchase orders, and vendor invoices. The system automatically generates an exception report of unmatched items. The exceptions are then reviewed and cleared by the accounts payable department. This control has two elements (1) the automated three-way match and (2) the manual review by the accounts payable department. The automated and manual control elements must be evaluated separately using the appropriate test guidance.

Testing of Manual Controls

Tests of manual controls should include a mix of inquiry, observation, examination, or reperformance. Inquiry alone, however, does not provide sufficient evidence to support the operating effectiveness of a control. Effective testing will generally require examining a control at a particular location/business unit in different instances (referred to as "sampling"). Inherent to sampling is the risk that although management may find nothing amiss in the samples (resulting in a conclusion that a control is operating effectively), the control is not necessarily operating effectively at all times. Management should minimize this sampling risk by selecting an appropriate number of times to test (perhaps by considering the concepts of statistical sampling theory, although not necessarily applying statistical sampling). Sampling risk increases with the frequency of the control's activation. The extent of management's testing is based on its judgment and the level of assurance it expects to derive from the test. The following table represents our view of the extent of testing necessary to support a conclusion that a manual control is operating effectively, provided no exceptions are found:

Frequency of Manual Control's Performance	Typical Number/Range of Times to Test Controls	Factors to Consider When Deciding the Extent of Testing
Annually	1	■ Complexity of the control ■ Significance of judgment in the control operation ■ Level of competence necessary to perform the control ■ Frequency of operation of the control ■ Impact of changes in volume or personnel performing the control ■ Importance of the control ● Addresses multiple assertions ● Period-end detective control ● Only control that covers a particular assertion
Quarterly	2	
Monthly	2 to 5	
Weekly	5 to 15	
Daily	20 to 40	
Multiple Times a Day	25 to 60	

The sample size that management decides to select for testing should be based on the significance of the control in question and the level of assurance desired. The fewer items tested, the greater the risk of an incorrect conclusion. Thus, for highly critical controls, or when a single manual control provides the sole support for a financial statement assertion regarding a significant account, we believe management should consider increasing its sample size to the high end of the range provided in the table above. This decision should be made after considering other evidence available to management (e.g., results of self-assessment, testing by internal audit, or evidence from other monitoring controls). The combination of evidence should provide management with a high level of assurance the control is operating effectively. When no exceptions are found, these sample sizes will provide management with a high level of assurance that the control is operating effectively. For example, (using the concepts of statistical sampling theory) if 25 instances of a control (occurring multiple times a day) are tested and no exceptions are found, there is a 90 percent confidence level that the actual exception rate is no more than 9 percent. If 60 instances are tested with no exceptions, there is a 95 percent confidence level that the actual exception rate is no more than 5 percent.

FAQ: What areas should a company test within each of the remaining four components of internal control (i.e., excluding control activities)?

The testing plan for the remaining four components of internal control of the COSO framework should include, at a minimum, the evaluation of each of the sub-components that were discussed in Section III – Scoping and Planning: The Beginning of an Effective Project. Examples of testing procedures may include:

Control Environment

- *Evaluate the "tone at the top" through inquiry, observation, focus groups, and surveys*
- *Obtain an understanding of, observe, and evaluate the process for handling exceptions to the company's code of conduct*
- *Review the documented authorization levels and assess their reasonableness compared to the positions and responsibilities of the individuals*
- *Examine job descriptions for key financial reporting positions and evaluate whether employee understanding of roles and responsibilities is consistent with the description*

Risk Assessment

- *Review management's process for evaluating risks, including assessing the likelihood of occurrence and determining needed actions*
- *Evaluate whether management adequately addresses how it will identify and analyze significant estimates recorded in the financial statements*

Information and Communication

- *Evaluate senior management's and the board's involvement in the development of the strategic plan for information systems, including appropriate allocation of resources*
- *Obtain an understanding of the process for updating the accounting policy manual for new pronouncements and how updates are distributed to the appropriate individuals*
- *Inquire as to the extent to which outside parties have been made aware of the entity's ethical standards and observe the process for addressing complaints from outside parties*

FAQ: What areas should a company test within each of the remaining four components of internal control (i.e., excluding control activities)? *Continued*

Monitoring

- *Obtain an understanding of the monthly financial statement analysis process and observe how significant or unusual items are investigated and resolved*
- *Evaluate the effectiveness of the internal audit function and the process for reporting and following-up on identified internal control deficiencies*

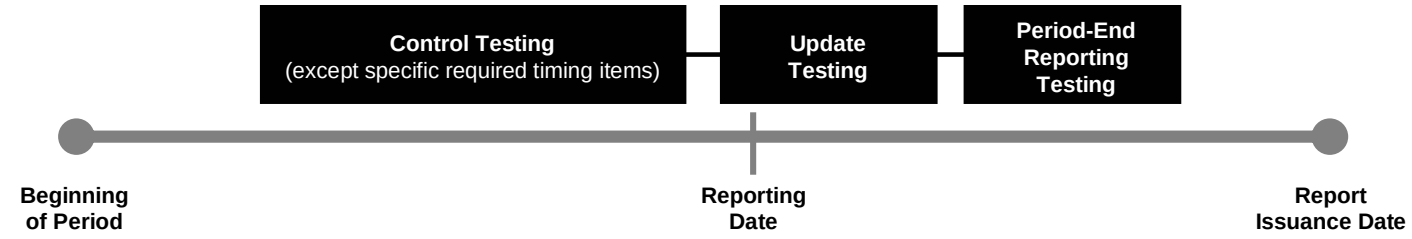
Additionally, management must test its anti-fraud programs, and the company must evaluate the effectiveness of the audit committee.

FAQ: How do sample sizes for the other four components of internal control compare with those for manual control activities outlined in the table above?

Tests of the other four components of internal control will typically consist of inquiry, observation, and/or examination. Sufficient evidence should be obtained that these control components are operating as designed. The sample sizes in the aforementioned table may not be appropriate due to the nature of controls being tested. The Standard indicates that in some cases documentary evidence of controls or their performance does not exist and is not expected to exist. In these cases, management would make inquiries and observation of activities to support the controls that are in place.

Timing of Procedures

The time period over which a company tests its internal control must be sufficient to determine operating effectiveness as of the end of the fiscal year. As previously stated, we believe it would be unwise and impractical for management to perform all testing as of the end of the fiscal year, and it would not allow management sufficient time to remediate deficiencies. The following illustration depicts the potential period over which management should conduct its testing.



Testing performed earlier in the year generally provides less evidence of effectiveness at the reporting date than testing performed later in the year and will require more extensive updating near year-end. For controls that cover (1) significant non-routine transactions, or (2) accounts or classes of transactions for which measurement involves a high degree of subjectivity or judgment, the company should perform testing closer to

or as of the reporting date rather than at an interim date. The timing of testing should allow sufficient time for any necessary remediation efforts.

Management's testing also encompasses controls that are relevant to the company's financial reporting, even though such controls may not operate until after the company's fiscal year-end. For example, some controls over the year-end closing process normally operate only after the reporting date. Accordingly, management's evaluation of the operating effectiveness of such controls occurs at the time that the controls are operating. Because testing these controls only in the year-end reporting process would not allow time to remediate any weaknesses, some companies are performing a "dry run" at an earlier quarter-end or month-end, with plans to repeat testing during the year-end closing process.

Decisions about updating should be based on the significance of the specific controls, the testing results, and the length of the remaining period after interim testing. Update procedures could include a combination of:

- Inquiries of personnel to verify that the controls tested during the interim period are still in place (this type of testing alone would not be sufficient)
- Observation of the control being performed
- Additional walkthroughs (i.e., inquiry and observation of one transaction through the process)
- Testing of additional samples for more important and pervasive controls

In situations where there have been significant changes in internal control during the year (e.g., changes that address deficiencies detected during interim testing), management must assess the operating effectiveness of the new controls between the time they were implemented and year-end. This period must be sufficient to enable management to obtain adequate evidence of the controls' operating effectiveness. For example, if a new monthly manual control is implemented in the middle of the fiscal year's last month, management may not have sufficient opportunity to assess its operating effectiveness.

Lessons Learned – Timing of Testing

Companies are using various techniques to spread their testing across the fiscal year. One method is to assess the sample over several quarters. For example, in order to reach a desired sample quantity of 60, management could test 15 instances in each quarter. The advantage of this technique is that management can obtain more frequent feedback on whether the control is working for purposes of the company's quarterly Section 302 certifications.

FAQ: How much documentation of tests of controls should management retain?

We believe management should base the level of documentation on an "experienced person approach." Since the documentation will provide the support for management's assertions, it will be reviewed by the external auditor and possibly by regulators. Thus, the testing should be sufficiently documented to allow an independent person to understand and reperform the test, including the identification of the items tested (for example, the title and date of the report, invoice numbers, check numbers), who performed the testing, the test results, and the overall conclusion. When samples are used, the basis for the sample size selection should also be documented. We believe documentation of management's assessment should be retained for seven years, consistent with the PCAOB's requirement of the external auditor.

Testing General Computer Controls

In virtually all companies, many of the controls that management relies on are automated or depend significantly on information systems and technology. As a result, management must evaluate the effectiveness of information technology general controls to ensure the continuous, effective operation of the automated/information technology dependent controls. Given the technical skills necessary to evaluate information technology general computer controls, management must determine whether the company has personnel with the necessary expertise to perform this work or whether it must engage a specialist. When testing general computer controls, management must also consider the impacts of implementing new accounting systems and the potential need to evaluate the new and old systems. The PCAOB staff has addressed this matter in Question 6 of its FAQs included in Appendix IX.

When evaluating and testing general computer controls, the following examples of factors should be considered by management with respect to each component of general computer controls as it relates to internal control over financial reporting (note that the information technology control environment should be assessed in a manner similar to the overall control environment):

Program Development

Control Objective: New systems and applications being developed are authorized, tested, approved, properly implemented, and documented.

Management should document, test, and evaluate the controls in place to ensure:

- new system developments and acquisitions are approved by an appropriate level of both information technology and business management
- the system development methodology had appropriate controls and is followed for development or acquisition of systems and applications utilized for financial reporting processes
- existing controls that are affected by the design and implementation of new systems are modified or redesigned to retain their integrity
- adequate testing is followed for all development of systems and applications utilized during financial reporting processes
- all testing is approved by both users and an appropriate level of information technology and business management
- appropriate system, user, and control documentation is developed for new systems and applications utilized during financial statement reporting processes
- the development of interfaces to ensure that data is transferred between applications accurately and completely
- restricted access for migrating new systems and applications into the production environment
- data migrated to the new application or system retains its integrity
- users are trained on new systems and applications in accordance with a defined training plan

Program Changes

Control Objective: Changes to existing systems and applications are authorized, tested, approved, properly implemented, and documented.

Management should document, test, and evaluate the controls in place to ensure:

- any changes to the systems and applications providing control over financial reporting have been properly authorized by appropriate management
- system, user, and control documentation is modified to properly reflect changes to systems relevant for financial reporting
- changes to applications and systems are tested with test results documented
- restricted access for migrating changes to systems and applications into the production environment
- unauthorized changes are not made to system files for applications, subsequent to migration into production
- all authorized changes to systems and applications are migrated to the production environment
- users are trained on changes to systems and applications

Access to Programs and Data (Security)

Control Objective: Logical access to system resources (for example programs, data, tables, and parameters) is restricted to properly authorized individuals for applications, databases, operating systems, and networks.

Management should document, test, and evaluate the controls in place to ensure:

- information security is managed to guide consistent implementation of security practices
- users are aware of the organization's position with regard to information security as it pertains to financial reporting data
- logical access to information technology computing resources is appropriately restricted by the implementation of identification, authentication, and authorization mechanisms
- procedures have been established so that user accounts are added, modified, and deleted in a timely manner
- appropriateness of access rights is periodically reviewed
- an effective mechanism is in place to log security activity, identify potential violations, and escalate and act upon them in a timely manner

Computer Operations

Control Objective: System and application processing are appropriately authorized and scheduled and processed deviations or problems from scheduled processing are identified and resolved.

Management should document, test, and evaluate the controls in place to ensure:

- appropriate backup and recovery procedures exist so that data, transactions, and programs that are necessary for financial reporting can be recovered
- effective procedures exist and are followed to periodically test the effectiveness of the restoration process and the quality of backup media
- only authorized individuals have access to the back-up media
- problem management procedures are effective to record, analyze, and resolve incidents, problems, and errors for systems and applications in a timely manner
- system jobs, including batch jobs and interfaces, for relevant financial reporting applications or data are processed accurately, completely, and in a timely manner

FAQ: To fulfil Section 404's requirements regarding the safeguarding of assets, must management test controls that ensure the continuity of operations?

No. The Standard clearly states that a company's business continuity or contingency plans have no effect on its current ability to initiate, authorize, record, process, or report financial data. However, we believe a daily backup procedure (such as storing tapes in an offsite location to ensure recovery if a file is lost or destroyed) is an information technology general computer control that should be addressed in management's assessment of internal control over financial reporting. While such a procedure may support a company's business continuity plan, it also provides an important financial reporting control. It is not uncommon for data to be lost or corrupted during the daily processing of financial information. Appropriate backup and recovery procedures allow for proper control over the restoration process, ensuring the integrity of the information.

Evaluate the Test Results

The objective of evaluating test results is to conclude whether the controls are **operating effectively** to support the financial statement assertions**.** For example, consider the review and sign-off of a reconciliation of a subsidiary ledger for sales to the general ledger. Management must conclude, on the basis of the testing performed, whether the control effectively supports the completeness assertion. Other controls in the sales process would be tested to ensure that all sales transactions have been posted in the subsidiary ledger to support further the completeness assertion. And, still other controls would be tested to support the other relevant assertions such as valuation, existence, rights and obligations, and presentation and disclosure. When evaluating the results and related evidence of specific tests, the following questions may be useful for consideration:

- What risk is the control intended to mitigate?
- Were exceptions found?
- Were exceptions resolved?
- Is there a process for correcting recurring exceptions?

In general, controls are tested on an accept/reject basis (i.e., a control is either working reliably or it is not). Also, a high level of assurance that controls are working effectively is required. To attain a high level of assurance regarding the operating effectiveness of a control, no more than a negligible exception rate can be accepted.

If an exception occurs in testing, management must evaluate the exception to determine why it occurred. Upon investigation of the exception, management may determine that the control is not operating effectively.

Alternatively, the results of the investigation may not be conclusive that a deficiency exists. In this circumstance, assuming the control operates at least daily, management may select and test another sample of equal size. If no exceptions exist in the second sample, a conclusion that the overall exception rate is no more than negligible would typically be appropriate. In this case, the exception would not be considered a deficiency as the likelihood of misstatement is not more than remote. The PCAOB staff has also clarified in its FAQs (refer to Question 13 in Appendix IX) that controls with observed non-negligible deviation rates are deficiencies. When an exception occurs in a quarterly, monthly, or weekly control, we believe there is a strong indication that a deficiency exists due to the small populations involved (i.e., four quarters, 12 months, or 52 weeks). Additionally, the existence of compensating controls does not effect whether an internal control deficiency exists (refer to Question 12 in Appendix IX).

Management should develop an inventory of all internal control deficiencies, significant deficiencies, and material weaknesses. The root cause for each deficiency should be documented and an assessment of the necessary corrective action made (e.g., redesign the control or retrain the individuals involved). The project leaders and/or steering committee should carefully assess each deficiency and prioritize remedial actions. Each remediated control will need to be retested to verify operating effectiveness.

FAQ: How long must a remedied control operate before it can be concluded that the control is operating effectively?

We believe the necessary length of time a control must be operating will depend on the frequency of the control's operation. The more often a control is performed, the shorter the time management will need to gather sufficient evidence that the control is operating effectively, as illustrated by the table below.

Frequency of Control	Suggested Time Period of Operation Prior to the Reporting Date
Quarterly	2 quarters*
Monthly	2 months
Weekly	5 weeks
Daily	20 days
Multiple Times per Day	25 times over a multiple day period

**Includes the fourth quarter as one of the quarters.*

Lessons Learned – Plan for Deficiencies and Remediation

In working with companies in readiness projects, we have found that management's testing will invariably uncover deficiencies that require remediation. Management should take this into account when developing the project plan by estimating that a certain percentage of controls will have to be remediated and re-tested.

SECTION VII: Evaluation of Internal Control Deficiencies and Reporting

Evaluating the significance of internal control deficiencies and reporting is an evolving area that will require a significant degree of management judgment.

Significance of Internal Control Deficiencies

Control deficiencies can range from internal control deficiencies to significant deficiencies to material weaknesses in internal control. These are defined in the Standard as follows:

- **Internal Control Deficiency** — Exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.
- **Significant Deficiency** — An internal control deficiency or combination of control deficiencies that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with GAAP such that there is a more-than-remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.

  The Standard specifies that a misstatement is **inconsequential** if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when combined with other misstatements, would **clearly be immaterial** to the financial statements. If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement would be **more than inconsequential**.
- **Material Weakness** — A significant deficiency or combination of significant deficiencies that results in a more-than-remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected.

The term *remote likelihood,* as used in the definition of significant deficiency and material weakness, has the same meaning that the term *remote* has in FASB Statement No. 5 (FAS 5), *Accounting for Contingencies*. In FAS 5, the term *remote* means that "the chance of the future event or events occurring is slight."

The following criteria can be used to assess the classification of an internal control deficiency, individually or in the aggregate, **after considering compensating controls**:

Classification of Deficiency	Likelihood of Misstatement		Potential Magnitude of Misstatement
Significant Deficiency	More than remote	AND	More than inconsequential
Material Weakness	More than remote	AND	Material

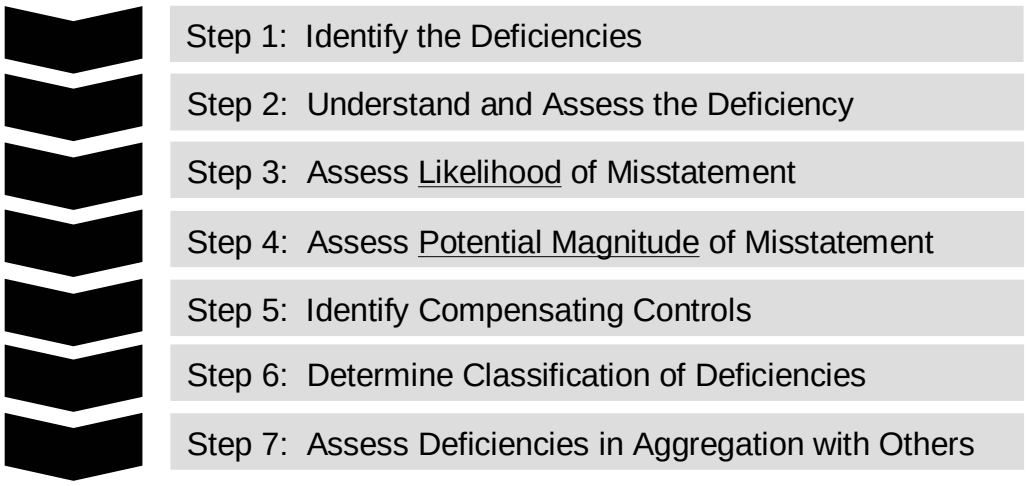
FAQ: What is the meaning of inconsequential?

We believe the Standard's definition of when a misstatement is more than inconsequential (i.e., clearly immaterial to the financial statements) does not mean that if 5 percent of pre-tax income (loss) is material, then 3 percent of pre-tax income (loss) is "clearly immaterial." Rather, we believe the use of "inconsequential" sets a relatively low hurdle and based on the limited guidance on the subject, would not typically exceed 0.5 to 1 percent of pre-tax income (loss) and could be lower depending on qualitative factors.

The PCAOB staff has indicated that the definition of significant deficiency is not, by definition, equivalent to aggregating likely misstatements from the audit of the financial statements. Rather, it should be based upon the combination of concepts from both Staff Accounting Bulletin No. 99, Materiality*, and AU Section 312,* Audit Risk and Materiality in Conducting an Audit. *Further discussion is included in Question 11 of the PCAOB staff's FAQs included in Appendix IX.*

The Process for Identifying, Assessing, and Classifying Internal Control Deficiencies

Although there are many ways to identify, assess, and classify internal control deficiencies, we believe the following steps provide a reasonable approach:



Step 1: Identify the Deficiencies

Internal control deficiencies may relate to the design or operating effectiveness of a control. Management must consider deficiencies identified in all areas, including each of the five components of internal control, company-level controls, anti-fraud programs, and audit committee effectiveness. Deficiencies may be identified through many sources, including:

- management through its assessment of internal control over financial reporting
- management in a self-assessment process
- internal audit in the scope of its work

- the external auditors in the scope of their work
- service organization SAS 70 reports
- regulatory inspections

Step 2: Understand and Assess the Deficiency

Management should ensure that it has an accurate understanding of the nature and implications of the deficiency, as well as its potential impact on the financial statements. A focus on the financial statement assertion(s) that is not being supported as a result of the deficiency will assist in this understanding.

Step 3: Assess Likelihood of Misstatement

The determination of likelihood is based on the potential that a misstatement would not be prevented or detected, not on whether a misstatement **has** occurred. Deficiencies for which there is only a remote likelihood of occurrence cannot rise to the level of a significant deficiency or material weakness, and thus evaluation of the magnitude of a potential misstatement (Step 4) is not required.

The Standard indicates the following factors may impact likelihood:

Likelihood
■ *The nature of the financial statement accounts, disclosures, and assertions involved;*
■ *The susceptibility of the related assets or liability to loss or fraud (that is, greater susceptibility increases risk);*
■ *The subjectivity, complexity, or extent of judgment required to determine the amount involved (that is greater subjectivity, complexity, or judgement, like that related to an accounting estimate, increases risk);*
■ *The cause and frequency of known or detected exceptions for the operating effectiveness of a control;*
■ *The interaction or relationship of the control with the other controls (that is, the interdependence or redundancy of the control);*
■ *The interaction of the deficiencies;*
■ *The possible future consequences of the deficiency.*

Step 4: Assess Potential Magnitude of Misstatement

Quantifying the impact of internal control deficiencies is difficult. Management should consider the total account balance or transaction flow, and the assertion that is exposed to risk as a result of the deficiency. The focus should be on the size of the **potential** error that could occur in a more-than-remote likelihood situation. Accordingly, management must address whether the potential magnitude of the deficiency is more than inconsequential or material. The Standard indicates the following factors may impact the magnitude:

Magnitude
■ *The financial statement amounts or total of transactions exposed to the deficiency;* ■ *The volume of activity in the account balance or class of transactions exposed to the deficiency that has occurred in the current period or that is expected in future periods.*

Step 5: Identify Compensating Controls

Control deficiencies should first be evaluated individually or in combination and then the determination of whether they are significant deficiencies or material weaknesses should be made considering the effects of compensating controls. Compensating controls should be taken into account when assessing the likelihood of a misstatement occurring and not being prevented or detected. In addition, a compensating control may limit the potential magnitude of a deficiency (e.g., the compensating control only operates above a given dollar amount). However, the existence of a compensating control does not affect whether a control deficiency exists (refer to the PCAOB staff's Question 12 in Appendix IX)

If management believes there are compensating controls in place that could address the financial statement assertion or risk resulting from the deficiency, management should consider and validate whether

- the compensating control is effective
- the compensating control would identify an error and address the assertion

High-level analytical procedures are not sufficient to compensate for deficiencies. For a compensating control to be effective, the PCAOB staff has indicated that the compensating control should operate at a level of precision that would prevent or detect a misstatement that was more than inconsequential or material, respectively (refer to Question 14 in Appendix IX). Additionally, if a misstatement occurred as the result of a deficiency, it is presumed that the compensating control, if it was effective, should have prevented or detected the misstatement.

Step 6: Determine Classification of Deficiencies

Based on an assessment of the likelihood and magnitude of a misstatement resulting from an internal control deficiency, management should determine if the deficiency represents a significant deficiency or a material weakness. The Standard indicates that if the deficiency would prevent a prudent person from concluding that reasonable assurance exists that transactions are recorded to permit the preparation of the financial statements in conformity with GAAP, the deficiency should be at least a significant deficiency. SEC Staff Accounting Bulletin No. 99, *Materiality*, provides guidance about the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs.

The Standard indicates weaknesses in the following areas would ordinarily be considered at least significant deficiencies:

- Controls over the selection and application of accounting policies that are in conformity with GAAP
- Anti-fraud programs and controls
- Controls over non-routine or non-systematic transactions
- Controls over the period-end financial reporting process

The Standard indicates each of the following circumstances should be regarded as at least a significant deficiency, and as a strong indicator that a material weakness exists:

- Restatement of previously issued financial statements to reflect the correction of a misstatement due to error or fraud.
- Identification by the auditor of a material misstatement in the financial statements in the current period that was not initially identified by the company's internal control over financial reporting. (This would be a strong indicator of a material weakness even if management were to subsequently correct the misstatement.)
- Oversight of the company's external financial reporting and internal control over financial reporting by the company's audit committee is ineffective.
- The internal audit function or the risk assessment function is ineffective at a company for which such a function needs to be effective for the company to have an effective monitoring or risk assessment component, such as for very large or highly complex companies.
- For complex entities in highly regulated industries, an ineffective regulatory compliance function. This relates solely to those aspects of the ineffective regulatory compliance function in which associated violations of laws and regulations could have a material effect on the reliability of financial reporting.
- Identification of fraud of any magnitude on the part of senior management.
- Significant deficiencies that have been communicated to management and the audit committee remain uncorrected after some reasonable period of time.
- An ineffective control environment.

The PCAOB staff has provided further clarification when evaluating whether an auditor's finding of a material misstatement in the financial statements would constitute a material weakness (refer to Question 7 in Appendix IX). Refer to Appendix VII for additional examples of significant deficiencies and material weaknesses.

Step 7: Assess Deficiencies in Aggregation with Others

The Standard indicates that a significant deficiency can be a combination of internal control deficiencies, and a material weakness can be a combination of significant deficiencies. Thus, management must accumulate all internal control deficiencies for evaluation in the aggregate, considering whether there is a concentration of deficiencies over a particular business process, account, or assertion. For example, assume a particular location has three internal control deficiencies in relation to revenue processing. Although none of these deficiencies may individually be a significant deficiency, they could potentially rise to this level when aggregated. The assessment of the interaction of deficiencies with each other is essentially a search for patterns (e.g., could the deficiencies affect the same financial statement accounts and assertions).

FAQ: How should the company characterize and prioritize its identified internal control deficiencies?

There is no prescribed method to summarize deficiencies. We recommend the use of a corporate-wide tool to compile information about internal control deficiencies and prioritize their handling. In large, multinational organizations, the accumulation, characterization, and prioritization of control deficiencies will require considerable judgment. It is entirely possible that several hundred control deficiencies might be detected and require evaluation as a result of the internal control reviews that are conducted by management, internal audit, or outside service providers. Although management's assessment of internal control over financial reporting cannot be based on the external auditor's work, management should evaluate any deficiencies identified by the external auditor.

We believe that an effective process to communicate individual and combined deficiencies should be sufficiently robust to allow management to identify patterns of deficiencies across the business.

Reporting – Management

A company is required to include in its annual SEC filing (e.g., Form 10-K) management's report regarding internal control over financial reporting. The report must include the following:

- 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 assessment of the effectiveness of the company's internal control over financial reporting
- An 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 an explicit statement as to whether the internal control over financial reporting is effective
- A statement that the company's 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 company's internal control over financial reporting

Management is not permitted to conclude that its internal control over financial reporting is effective if there is one or more material weakness. Additionally, the SEC staff has indicated that management may not qualify its conclusion by stating that its internal control over financial reporting is effective with certain qualifications or exceptions or express similar positions (refer to Question 5 in SEC staff's FAQs in Appendix VIII). The Standard indicates that management may want to describe in its report any (1) corrective actions after the date of assessment, (2) plans to implement new controls, or (3) a statement that management believes the cost of correcting a material weakness would exceed the benefits to be derived from implementing new controls.

FAQ: What procedures should management use to address internal control on a quarterly basis?

After the registrant's first management report on internal control over financial reporting, pursuant to Item 308 of Regulations S-K or S-B, management is required to certify whether or not there were significant changes in internal control or in other factors that could significantly affect internal control subsequent to the date of the most recent evaluation, including any corrective actions with regard to significant deficiencies and material weaknesses (refer to Question 9 in the SEC staff's FAQs in Appendix VIII for further discussion). Management should implement procedures that will ensure the timely detection and reporting of material changes in internal control over financial reporting during the most recent fiscal quarter (the fourth fiscal quarter in the case of an annual report) that have materially affected, or are reasonably likely to materially affect the company's internal control over financial reporting. Changes in internal control might arise from the following:

- *Implementation of new systems*
- *Centralization or decentralization of accounting functions*
- *Changes in processes or employees' responsibilities*
- *Acquisitions or divestitures*
- *Changes in management*
- *Detection of fraudulent activities*

Auditor's Evaluation of Management's Report

The Standard requires the external auditor to opine on management's assessment of the effectiveness of internal control over financial reporting, stating that when auditors are evaluating management's assessment, they should consider the following questions:

- Has management clearly stated its responsibility for establishing and maintaining adequate internal control over financial reporting?
- Did management use a suitable framework for its assessment?
- Is management's assessment of the effectiveness of internal control over financial reporting free of material misstatement?
- Has management documented its assessment in an acceptable form?
- Did management properly disclose all detected material weaknesses?

The PCAOB staff has also indicated that the auditor can not issue an adverse opinion on management's assessment of its internal controls and an unqualified opinion on the effectiveness of internal control over financial reporting if management does not have a sufficient basis for its assessment of the effectiveness of internal control over financial reporting. The Standard requires that management fulfil its responsibilities in evaluating and supporting its assessment on the effectiveness of internal control over financial reporting. Refer to Question 8 in Appendix IX for the PCAOB staff's FAQ addressing this matter.

SECTION VIII: Communication – Important Observations

Communication among management, the audit committee, and the external auditor is an important part of the Section 404 project. This section explains required communications by management, what written representations management is required to submit to the external auditor, and what the auditor must communicate to management and the audit committee.

Required Communications by Management

Management must communicate all significant deficiencies and material weaknesses that it detects to the audit committee and the external auditor. These communications should be made at least quarterly.

Written Representations from Management to the Auditor

The Standard requires the auditor to obtain the following representations from management:

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

Required Communications by the Auditors

Before issuing an opinion, the auditor must report in writing to management and the company's audit committee all significant deficiencies and material weaknesses. The communication should distinguish clearly between those matters considered to be significant deficiencies and those considered to be material weaknesses.

In addition, the Standard requires the auditor to communicate in writing to the company's board of directors if a significant deficiency or material weakness exists related to the audit committee's oversight of the company's external financial reporting and internal control over financial reporting.

The auditor must also communicate to management, in writing, all deficiencies in internal control over financial reporting of a lesser magnitude than significant deficiencies identified during the audit, and inform the audit committee when such a communication has been made.

It is recommended that the external auditor communicate with management and the audit committee in a timely manner, as opposed to waiting until the audit engagement ends. This will ensure that (1) all necessary parties are kept informed of the audit's status and results and (2) the appropriate parties address the issues in a timely and adequate manner.

SECTION IX: Mergers and Acquisitions – Impact of the Sarbanes-Oxley Act

The Act does not explicitly mention mergers and acquisitions, making it easy to overlook any impact that the Act might have on them. However, acquisition-minded companies that fail to consider the Act's implications may be in for some unpleasant surprises. Since the certification and attestation requirements of Sections 302 and 404 apply to internal control over the company's entire financial statements – including acquisitions completed before the reporting date - the Act may have an impact on certain merger and acquisition processes for public companies. The practical impact for companies is that their Section 302 assessments will have to include acquired entities, beginning with the first quarter-end after the acquisition. Management must also consider the impact of acquisitions on its Section 404 assessment.

The SEC staff has indicated that management may exclude newly acquired entities from its assessment of internal control over financial reporting where it is not possible to conduct an assessment of the internal control of an acquired business in the period between the consummation date and the date of management's assessment. However this exclusion should not extend beyond one year from the date of acquisition. If a newly acquired entity is excluded from assessment, management must disclose this fact in its report and Form 10-K. The Standard provides that if the SEC permits management to limit its assessment with respect to certain entities, the auditor can do the same, however reference to the entity excluded from the scope must be made in the auditor's report. Refer to Question 3 in the SEC staff's FAQs included in Appendix VIII for further discussion.

Corporate development teams (i.e., teams responsible for identifying and analyzing potential acquisition candidates) start out with many questions about the Act, including:

- Should the company be concerned about Sections 302 and 404 vis-à-vis a given acquisition?
- How will the company accomplish compliance?
- Can the target comply on a stand-alone basis?

We believe the due diligence process will evolve over time, as practice provides a clearer view of the relative complexity and cost of implementing the Act. Some companies are already incorporating "readiness reviews" into their pre-closing due diligence procedures.

Should the company be concerned about Sections 302 and 404 vis-à-vis a given acquisition?

Knowing that management's certifications under Sections 302 and 404 of the Act will ultimately apply to acquisitions, corporate development teams should determine whether an acquisition warrants focus on internal control. The development team must consider

- the materiality of a target relative to the business (pro forma, including the acquisition), and
- the quantitative, as well as qualitative, elements of materiality.

For example, a target company may be very small compared with the acquirer, but bring the latter into a new, high-risk business. As a result, the acquirer may want to evaluate critically the target's internal control over the specific significant risks.

Based on materiality and other considerations, management will determine prior to closing how the target would fit into its scoping for Section 404. These considerations are the same as those discussed in greater detail in Section III, Scoping and Planning – The Beginning of an Effective Project.

How will the company accomplish compliance?

There are two ways that a target can comply with Section 404, neither of which is likely to be practical on its own. Under the first approach, the target would change virtually every control and process to make it compatible with the buyer's internal control. Of course, this presumes that the design and operation of the buyer's internal control are effective. Under the other approach, the acquirer would leave all the target's controls as they are and assess the effectiveness of their design and operation.

Most companies will use some combination of these approaches. Even if the intention is to incorporate the acquired entity into the buyer's financial systems, it is likely that the controls and processes that take place outside the computer system will be different at the target, at least initially.

Transition services agreements will influence a company's short- and long-term plans to comply with Section 404. Consider the purchase of an entity that has been carved out of a larger business. The purchase may come with an agreement that the seller will process sales and inventory transactions for some time. The buyer then outsources to the seller the controls around these areas; if the controls are significant, they must be tested by the buyer (which could include the seller providing the buyer a Type II SAS 70 report).

Companies may find that accelerating integration will benefit the economics of the business and help management meet the control objectives. More controls will be necessary for complex business processes than for streamlined processes.

Lessons Learned – Evaluating Acquisitions Cost/Benefit Assessment
Correcting some processes will be potentially quicker than working around them. The cost of designing, executing, and testing controls that navigate a convoluted process will factor into the cost/benefit decision related to streamlining an acquisition.

Can the target comply on a stand-alone basis?

Assume that a target is individually important to the buyer and that the buyer decides not to integrate the acquisition into its information technology and operational systems for some time. Where should the assessment of controls start? The logical starting point is with any work performed by the seller/target company in terms of considering and documenting controls. The level of work will likely depend on the profile of the target company and/or its parent company.

Lessons Learned – Due Diligence for Internal Control
Due diligence should include specific consideration of internal control. The extent of this assessment will be determined by the seller's internal control environment at the time of the acquisition and the buyer's plans to make changes to the acquired company's operations and, therefore, changes to the controls after the acquisition.

A buyer will want to include in the due diligence process procedures for assessing the target's internal control. The following chart outlines some of the executive-level considerations based on the buyer and target profiles.

Buyer	*Target*	*Potential Control Implications*	*Controls Diagnostic Will:*
Public	Public Company	Likely where functions are combined	Evaluate and build on seller's work
Public	Division of a Public Company	Likely where the target relied on corporate shared services and where functions are combined	Build on seller's work, but consider changes in controls
Public	Private Company	Probably significant	Probably start from scratch
Public	Foreign Public or Private Company (whole or division)	Probably significant	Probably start from scratch, as foreign (non-U.S.) registrant will not have considered the Act
Private with Likely Public Offering	Public Company	Probably significant if target is integrated into existing business	Combine the approaches above; time line determined by exit date

FAQ: How can a company take its initial assessment of risks and complexity a step further?

Most companies use the COSO framework to assess their internal control. As this monograph has already discussed, the COSO framework specifies five components of effective internal control.

An internal control diagnostic that is performed as part of a company's due diligence could include an assessment of the considerations that the COSO framework identifies for company-level controls. Because the control environment is the foundation for the other components of control, we believe that the diagnostic should focus on this area in particular. The control environment sets the "tone at the top", which in turn influences the control consciousness of the remainder of the organization. Going forward, companies may assess anti-fraud programs more frequently in due diligence and, in many cases, conduct more thorough background checks on key members of management.

FAQ: What tactics will companies use to handle the impact of the internal control assessment in their acquisition process?

Companies are now formulating their plans to integrate control assessments into their due diligence. They are also considering the impact that their assessment of controls will have on the timing of transactions. Below are steps that management should consider taking:

- *Requiring a robust discussion (across the executive, corporate development, and compliance management team) of the timing of transactions*
- *Changing the requirements regarding information and access to management in a due diligence process*
- *Tailoring the length of time it will spend on due diligence based on its initial assessments*
- *Considering robust internal control work (guided by the initial assessment) in the period between signing and closing. We may see this period lengthen when the readiness work (i.e., combining the target's internal control with the buyer's) will take longer than it has historically. We may also see companies that are subject to anti-trust reviews of mergers develop a "clean team" that can do controls work even while regulatory approval of the merger is outstanding.*
- *Closing transactions at the beginning, rather than the end, of a quarter in order to maximize the time to prepare for Section 302 and 404 certifications*

For material targets, corporate development teams are faced with the question of what can reasonably be done to consider internal control in the due diligence process. The first sections of this monograph demonstrate that a full assessment of internal control is a complex process. It is unlikely that buyers will want to commit significant resources early in the evaluation of a potential acquisition candidate. They may also not gain access to sufficient information at the target to assess controls completely. At the same time, companies will want to mitigate the risks of an adverse opinion regarding controls, so they will need some manner of evaluation.

Since the Act is new, corporate development professionals are only now developing their approaches. Individual approaches may differ, but we believe they should all start with an understanding of the risks associated with the target business. Companies have always focused their due diligence on risks but have put them in a context of valuation, generally based on the earnings of the target business. In response to the increased focus on controls, management can start by viewing the information it already has about the target company through the lens of internal control.

Definition of Key Terms

This monograph uses many key terms when discussing how management must evaluate its internal control over financial reporting.

Automated Controls

Automated controls encompass those control procedures performed by a computer.

Business Process or Business Cycle

A business process or business cycle is any sequence of transactions that enables a company to complete tasks and achieve its business objectives. These transactions may range, in order of complexity, from performing simple activities (such as processing invoices), to managing key elements of the business operations (such as a wholesaler's inventory management and distribution system), to executing functional tasks (such as maintaining an organization's financial records), to cross-functional elements (such as the business's human resources department).

Business Process/Cycle Risk Assessment

As part of the scoping exercises, management must identify the primary business processes/cycles. In order to evaluate the extent of documentation and testing over each business process/cycle, management should perform a risk assessment of each business process/cycle. This risk assessment involves the identification of relevant risks to achieving the financial reporting objectives related to each account affected by each business process/cycle. Higher risk processes/cycles will be subject to a greater extent of documentation and testing.

Company-Level Controls

Company-level controls are controls management has in place to provide assurance that appropriate controls exist throughout the organization, including at the individual locations or business units. The Standard describes company-level controls as including

- Controls within the control environment, including tone at the top, the assignment of authority and responsibility, consistent policies and procedures, and company-wide initiatives, such as codes of conduct and fraud prevention
- Management's risk assessment process
- Centralized processing and controls
- Controls to monitor other controls, including the activities of the internal audit function, the audit committee, and self-assessment programs
- The period-end financial reporting process
- Board approved policies that address the business's significant control and risk management practices

COSO Framework

The Standard states that when management assesses the effectiveness of the company's internal control over financial reporting, it must base the assessment on a suitable, recognized control framework that has been established by a body of experts. In accordance with the Standard, a body that devises a framework for internal control must follow due process by submitting the framework for public comment. In the United States, the most broadly accepted framework is the framework that the COSO presented in its publication *Internal Control – Integrated Framework* in the early Nineties. Although the SEC staff has stated that the COSO framework satisfies the SEC's criteria, the Commission has not mandated its use. The SEC recognizes that there are other evaluation standards outside the United States and that other suitable frameworks may be developed within the United States. The SEC has stated that *Guidance on Assessing Control*, published by the Canadian Institute of Chartered Accountants, and the *Turnbull Report,* published by the Institute of Chartered Accountants in England & Wales, are examples of other suitable frameworks. The guidance in this monograph is premised on entities using the COSO framework.

COSO defines internal control as a process (one effected by an organization's board of directors, management, and other personnel) that is designed to provide reasonable assurance of an organization's achieving its objectives in three areas: (1) effective and efficient operations; (2) reliable financial reporting; and (3) compliance with applicable laws and regulations. Following are additional considerations as they relate to the application of these three COSO objectives to Section 404:

1. ***Effective and efficient operations:*** This area encompasses a company's basic business objectives, including performance and profitability goals and the safeguarding of assets. Section 404 generally does not cover objectives regarding effective and efficient operations, except as they relate to safeguarding assets.

2. ***Reliable financial reporting:*** Under the COSO framework, reliable financial reporting pertains to a company's preparation of financial statements and related notes in conformity with GAAP.

3. ***Compliance with applicable laws and regulations:*** The COSO framework covers controls for complying with regulations such as the Sarbanes-Oxley Act and related rules, so that companies can avoid damage to their reputation or other negative consequences. Section 404 does not address compliance with laws and regulations, except for compliance with rules directly related to financial statement preparation, such as the SEC's financial reporting requirements and the Internal Revenue Code.

Although the COSO framework addresses internal control over compliance and operations, **Section 404 generally requires management to assess only its internal control over financial reporting.** Thus management need not assess internal control over operations and compliance unless there are material financial reporting implications.

The COSO framework presents five interrelated components, each spanning the three objectives. Based on a company's size and structure, a company may implement the components differently; however, each component is relevant to all companies. Thus, when evaluating its internal control, management must consider each component. Discussion of the five components of internal control is as follows:

Control Environment: The control environment sets the tone for the organization, influencing the control consciousness of its people. This component is the foundation for all other components of internal control, providing discipline and structure. The control environment encompasses the following factors:

- Integrity and ethical values (including code of conduct and anti-fraud programs)
- Commitment to competence and development of people
- Management's philosophy and operating style
- Organizational structure
- Assignment of authority and responsibility
- Human resources policies and procedures
- Participation by those charged with governance (as required by the PCAOB, participation involves, among other things, the Board of Directors' assessment of the effectiveness of the audit committee)

Risk Assessment: Every entity faces a variety of risks from external and internal sources that must be assessed. Risk assessment is the identification and analysis of relevant risks and their impact on the achievement of the company's objectives. Management must form a basis for determining how risk should be managed. Because economic, industry, regulatory, and operating conditions will continue to change, management will need to employ mechanisms that enable management to identify and address the special risks that result from such change.

Control Activities: Control activities help ensure that management's directives are implemented and that necessary actions are taken to address risks, thus enabling the entity to achieve its objectives. These activities take place throughout the organization, at all levels, and in all functions, involving processes as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, the security of assets, and the segregation of duties.

Information and Communication: Pertinent information must be selected and communicated in a manner and time frame that enables people to carry out their responsibilities. Information systems produce reports containing operational, financial, and compliance-related information to enable management to run and control the business. This component includes not only internally generated data, but also information regarding external events, activities, and conditions necessary for informed decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across, and up the organization. Top management must clearly convey to all personnel that its control responsibilities must be taken seriously. Personnel must understand their role in the internal control system, as well as how their individual activities relate to the work of others. Personnel must also have a means of communicating significant information further up in the organization, and there must be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Monitoring Controls: The quality of internal control systems must be monitored, either continuously or periodically. Ongoing monitoring occurs in the course of operations and includes regular management and supervisory activities and other actions personnel take in performing their duties. The scope and frequency of management's separate evaluations will depend primarily on an assessment of (1) risks and (2) the effectiveness of ongoing monitoring procedures.

COSO uses a matrix (shown below) to illustrate the direct relationship between a company's objectives and control components. The third dimension of the matrix shows an entity's units or activities that relate to internal control.

An example of a component that spans each objective is financial and non-financial information that is generated from internal and external sources (i.e., the information and communication component) and is needed for the effective management of a company's resources, the development of reliable financial reporting, and compliance with laws and regulations.

Design Effectiveness

Internal control over financial reporting is designed effectively when the controls in place would meet the control objectives and be expected to prevent or detect errors or fraud that could result in material misstatements in the financial statements.

Detective Control

Detective controls have the objective of detecting errors or fraud that have already occurred that could result in a misstatement of the financial statements.

Disclosure Committee

The SEC has recommended that each public issuer create a disclosure committee. We believe this committee should report to senior management, including the chief executive officer and chief financial officer and would be responsible for:

- evaluating internal control over financial reporting and the accuracy of external reporting
- reviewing filings and evaluating items of interest
- reviewing analyst and press reports, SEC comment letters and company responses, SEC filings of industry peers, results of prior investigations, and statements by whistleblowers or disgruntled employees
- considering the materiality of information and determine disclosure obligations on a timely basis

The committee's composition may include representatives from accounting, treasury, internal audit, office of general counsel, significant business units, investor relations, and risk management. The committee should communicate orally or in writing to the chief financial officer and chief executive officer that no material information is excluded from the financial statements.

Financial Statement Assertions

Management and the auditor must document and test internal control over relevant financial statement assertions. AU 326 and the PCAOB define assertions as representations by management that are embodied in the financial statement components and can be classified in the following broad categories:

- Existence or Occurrence: This assertion addresses whether assets or liabilities of the entity exist at a given date and whether recorded transactions have occurred during a given period. For example, management asserts that finished goods inventories in the balance sheet are available for sale. Similarly, management asserts that sales in the income statement represent the exchange of goods or services with customers for cash or other consideration.

- Completeness: This assertion addresses whether all transactions and accounts that should be presented in the financial statements are so included. For example, management asserts that all purchases of goods and services are recorded and are included in the financial statements. Similarly, management asserts that notes payable in the balance sheet include all such obligations of the entity.

- Valuation or Allocation: This assertion addresses whether asset, liability, equity, revenue, and expense components have been included in the financial statements at appropriate amounts. For example, management asserts that property is recorded at historical cost and that such cost is systematically allocated to appropriate accounting periods. Similarly, management asserts that trade accounts receivable included in the balance sheet is stated at net realizable value.

- Rights and Obligations: This assertion addresses whether assets are the rights of the entity and liabilities are the obligations of the entity at a given date. For example, management asserts that amounts capitalized for leases in the balance sheet represent the cost of the entity's rights to leased property and that the corresponding lease liability represents an obligation of the entity.

- Presentation and Disclosure: This assertion addresses whether particular components of the financial statements are properly classified, described, and disclosed. For example, management asserts that obligations classified as long-term liabilities in the balance sheet will not mature within one year. Similarly, management asserts that amounts presented as extraordinary items in the income statement are properly classified and described.

Although the financial statement assertions appear to be similar to the information processing objectives/ CAVR, there is not a one-for-one relationship, and they are used for different purposes. Information processing objectives/CAVR are used to evaluate the design effectiveness of controls, particularly application controls, within a business process. Assertions are representations by management as to the fair presentation of the financial statements.

Some professional auditing standards, such as the International Standards on Auditing, include more than five financial statement assertions. Some companies are using fewer than five assertions when making their assessment. The PCAOB staff's FAQs indicate that management is not required to use the five assertions described in the Standard. If different assertions are used, the FAQs indicate that the auditor would be required to determine that he/she has identified and tested controls over all sources of potential misstatement

in each significant account and over all representations by management that have a meaningful bearing on whether an account is fairly stated (refer to Question 10 in Appendix IX).

General Computer Controls

General computer controls are one of the types of information processing controls included in the internal control component of control activities. These are the processes and procedures that are used to manage and control a company's information technology activities and computer environment. They are commonly divided into the following domains:

Domain	Definition	Typical Key Sub-components
Information Technology Control Environment	The information technology control environment is the extension of the overall control environment component into the information technology organization. This represents the "tone at the top" of the information technology organization and would be assessed in a similar way to the control environment of the company as a whole.	■ Each of the seven sub-components of the control environment, as they apply to the information technology organization: ● Integrity and ethical values ● Commitment to competence and development of people ● Management's philosophy and operating style ● Organizational structure ● Assignment of authority and responsibility ● Human resources policies and procedures ● Participation by those charged with governance
Program Development	The processes and controls used by a company to develop, configure, and implement new applications in order to meet the company's financial, operational, and compliance business objectives. This process is often referred to as the Software Development Lifecycle.	■ Program management of development activities ■ Project initiation (project planning, scope definition, and approval requirements) ■ Analysis and design, including business and technical specifications ■ Software/hardware package selection procedures ■ Testing and quality assurance ■ Data conversion ■ "Go-live" procedures ■ User and technical documentation and training

Domain	Definition	Typical Key Sub-components
Program Changes	The processes and controls used by a company to ensure that modifications to programs continue to meet the company's financial, operational, and compliance business objectives.	■ Management of program change activities ■ Specification, authorization, and tracking ■ Construction, including development environments and source code controls ■ Testing and quality assurance ■ Authorization to live environment ■ User and technical documentation and training
Access to Programs and Data (Security)	The processes and controls in place to ensure that access to system resources and data is authenticated and authorized to meet the company's financial, operational, and compliance business objectives.	■ Policies and procedures ■ Organization and management ■ Application security administration ■ Data security administration ■ Operating system security administration ■ Internal network security ■ Perimeter network security ■ Physical security
Computer Operations	The processes and controls in place over the day-to-day operations of the information technology systems and applications to ensure that production systems are able to meet financial, operational, and compliance business objectives.	■ Policies and procedures ■ Organization and management ■ Scheduling and batch processing ■ Backup management ■ Recovery procedures from operational failure

Information Processing Objectives/CAVR

The four information processing objectives (completeness, accuracy, validity, and restricted access – sometimes referred to as "CAVR") are a standard means to assess the integrity of the data that flows through a process. The four components of CAVR are listed below.

Information Processing Objective	Definition
Completeness	■ All recorded transactions are accepted by the system (only once). ■ Duplicate postings are rejected by the system. ■ Any transactions that are rejected are addressed and fixed.
Accuracy	■ Key data elements for transactions (including standing data) that are recorded and input to the computer are correct. ■ Changes in standing data are accurately input.
Validity	■ Transactions, including the alteration of standing data, are authorized. ■ Transactions, including standing data files, are not fictitious and they relate to the business.
Restricted Access	■ Unauthorized amendments of data are barred from the system. ■ The confidentiality of data is ensured. ■ Company assets are physically protected from theft and misuse. ■ The segregation of duties is ensured.

Internal Control Deficiency

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

A deficiency in *design* exists when (a) a control necessary to meet the control objective is missing or (b) an existing control is not properly designed so that, even if the control operates as designed, the control objective is not always met.

A deficiency in *operation* exists when a properly designed control does not operate as designed, or when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively.

Internal Control over Financial Reporting

The Standard defines internal control over financial reporting as a process designed by, or under the supervision of, the company's principal executive and principal financial officers, or person 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 GAAP. This process involves the maintenance of records; the recording of transactions; and the prevention/detection of unauthorized acquisition, use, or disposition of the company's assets.

Locations or Business Units

The majority of companies are comprised of more than one location or business unit. The definition of a location or a business unit will depend on the nature of the company. A location may be a legal entity (e.g., a subsidiary, partnership, limited liability company, etc.), a division, a reporting unit, or an operational facility (e.g., a plant or sales office). When completing management's Section 404 requirements, significant judgment must be applied in assessing the definition of a location or a business unit to ensure appropriate scoping of the project.

Manual Controls

Manual controls encompass those controls performed manually, not by computer systems.

Material Weakness

A material weakness is a significant deficiency (or a combination of significant deficiencies) that results in a more-than-remote likelihood that a material misstatement of the annual or interim financial statements will not be prevented or detected. The PCAOB has further clarified the definition of a material weakness in its FAQs (refer to Question 15 in Appendix IX).

Operational Effectiveness

Internal control over financial reporting is operating effectively when a properly designed control is operating as designed and the individual performing the control possesses the necessary authority and qualifications to perform the control effectively.

Preventive Control

Preventive controls have the objective of preventing errors or fraud from initially occurring that could result in a misstatement of the financial statements.

Section 404 Project/Assessment

The Section 404 Project is referred to in this monograph as those activities in which management will plan, document, test, and assess its internal control over financial reporting in accordance with Section 404 of the Act.

Significant Account and Disclosure

An account or disclosure is significant if there is a more-than-remote likelihood that the account or disclosure could contain misstatements that individually, or when aggregated with others, could have a material effect on the financial statements, considering the risks of both overstatement and understatement.

Significant Deficiency

A significant deficiency is a control deficiency (or combination of internal control deficiencies) that adversely affects the company's ability to initiate, authorize, record, process, or report external financial data reliably in accordance with GAAP such that there is a more-than-remote likelihood that a misstatement of the company's annual or interim financial statements that is more than inconsequential will not be prevented or detected.

The Standard specifies that a misstatement is inconsequential if a reasonable person would conclude, after considering the possibility of further undetected misstatements, that the misstatement, either individually or when combined with other misstatements, would clearly be immaterial to the financial statements. If a reasonable person could not reach such a conclusion regarding a particular misstatement, that misstatement would be more than inconsequential.

Sub-process or Sub-cycle

A sub-process or sub-cycle is a group of transactions for which specific accounting procedures and controls are established by an entity's management. For example, a revenue and receivables business process may include sub-processes, such as invoicing, pricing, or processing of cash receipts.

Walkthrough

A walkthrough is the process in which a transaction is traced from origination through the company's information systems until the transaction is reflected in the company's financial reports. A walkthrough should encompass the entire process of initiating, authorizing, recording, processing, and reporting individual transactions and controls for each significant process, including controls to address the risk of fraud.

Appendices

Appendix I – Examples of Business Processes/Cycles and Sub-Processes/ Sub-Cycles

BUSINESS PROCESSES/CYCLES AND SUB-PROCESSES/SUB-CYCLES
Inventory and Production
Inventory master file maintenance
Inventory quantity control
Obsolete and slow-moving inventory control
Shipping activities
Production activities
Receiving activities
Inventory costing
Purchasing
Vendor master file maintenance
Requisitions
Purchase orders
Goods receipting
Invoice processing
Cash disbursements
Revenues
Customer master file maintenance
Pricing and order processing
Invoicing
Credit and collections
Returns
Cash application and receipts processing
Revenue recognition
Incentive programs
Payroll and Employee Benefits
Payroll and employee master file maintenance
Time and attendance
Processing payroll
Pension and post retirement benefits
Management incentive and stock option programs
Capital Spending and Maintenance
Capital master file maintenance
Capital acquisition requests
Depreciation
Disposals
Leases (operating, capital)

BUSINESS PROCESSES/CYCLES AND SUB-PROCESSES/SUB-CYCLES
Financial Reporting (including period-end reporting)
Planning, budgeting, and management reporting
General ledger maintenance
Consolidation and adjusting, eliminating and consolidating entries
Accounting policies and procedures
Footnote support
Account analysis and reconciliations
Currency translation
Inter-company accounts
Adoption of new accounting pronouncements
Treasury and Risk Management
Debt and related interest
Cash
Investments and related interest
Equity
Hedging and derivatives
Workers compensation and other self-insurance programs
Legal exposures
Environmental exposures
Guarantees and other commitments
Taxes
Income taxes (local, state and federal)
- effective tax rate
- valuation allowances
- tax contingency considerations
Sales taxes
Property taxes
Information Systems
Control environment
Program development
Program changes
Access to programs and data (security access)
Computer operations
Other/Miscellaneous
Restructurings and impairments
Prepaids and other miscellaneous assets
Other miscellaneous liabilities and accruals
Equity method investments
Miscellaneous other income and expense
Purchase accounting
Discontinued operations

Appendix II — Example of Financial Statement Mapping of Significant Accounts to Business Processes/Cycles

Financial Statement Account	Consolidated Balance	404 Coverage	Percent Coverage	Corresponding Cycle	Corresponding Cycle	Corresponding Cycle
BALANCE SHEET, As of December 31, 200X						
Assets						
Cash & cash equivalents				Treasury and risk management	Revenue	Purchasing
Short-term investments				Treasury and risk management		
Accounts receivable, net				Revenue		
Prepaid expenses, deferred tax assets and other				Purchasing	Financial reporting	Taxes
Liabilities & Equity						
Current portion of capital lease obligations				Capital spending and maintenance		
Accounts payable				Purchasing	Financial reporting	
Accrued expenses				Purchasing	Financial reporting	Taxes
Accrued compensation				Purchasing	Financial reporting	Payroll and employee benefits
Current portion of restructuring				Asset management	Financial reporting	
INCOME STATEMENT, for year ended December 31, 200X						
Product sales				Revenue		
Maintenance revenue				Revenue		
Service revenues				Revenue		
Cost of goods sold				Purchasing	Payroll and employee benefits	
Payroll				Payroll and employee benefits		
Supporting Technology Controls						
Control environment				Information systems		
Program development				Information systems		
Program changes				Information systems		
Access to programs and data (Security)				Information systems		
Computer operations				Information systems		

Financial Statement Account	Consolidated Balance	404 Coverage	Percent Coverage	Corresponding Cycle	Corresponding Cycle	Corresponding Cycle
Note 1. The company						
Description of company updated for significant developments, such as acquisitions				Financial reporting		
Note 2. Summary of significant accounting policies						
Company has summarized its significant policies around ■ Principles of general ledger accounting ■ Management estimates and assumptions				Financial reporting		
Note 3. Investments						
Company provides detail of investments and debt securities classified as available for sale				Financial reporting	Treasury and risk management	
Note 4: Goodwill and intangible assets						
Company provides summary of goodwill and intangible assets which includes impairment testing				Financial reporting	Miscellaneous	
Note 19. Subsequent events						
Company discloses any material subsequent events				Financial reporting	Treasury and risk management	
Other 10K disclosures						
Financial statement schedules				Financial reporting	Treasury and risk management	

Appendix III — Example of Mapping Business Processes/Cycles and Sub-Processes/ Sub-Cycles to Locations

Business Process Cycle	Business Unit	Sub-Process 1	Sub-Process 2	Sub-Process 3	Sub-Process 4	Sub-Process 5	Sub-Process 6	Sub-Process 7
Revenue	**Corporate**	Customer master	Pricing	Order processing	Invoicing	Credit and Collections		Cash application
	Europe	Customer master		Order processing			Returns	
Inventory and Production	**Corporate**		Obsolescence			Costing	Master file	
	Europe	Quantity control		Shipping	Receiving			
Purchasing	**Corporate**	Vendor maintenance	Requisitions	Purchase orders	Goods receipting	Invoice processing	Cash disburse-ments	
	Europe	Vendor maintenance	Requisitions	Purchase orders	Goods receipting	Invoice processing	Cash disburse-ments	
Treasury and Risk Management	**Corporate**	Cash management	Investment management	Hedging and derivatives	Insurance	Legal	Environ-mental	Guarantees/ Commitments
	Europe	Cash management			Insurance		Environ-mental	Guarantees/ Commitments
Capital Spending and Maintenance	**Corporate**	Acquisition requests	Master file	Depreciation	Disposals	Leases	Physical maintenance	
	Europe	Acquisition requests	Master file	Depreciation	Disposals	Leases	Physical maintenance	
Payroll and Employee Benefits	**Corporate**	Master file	Time and attendance	Processing payroll	Pension and post retirement	Management incentives and stock compensa-tion		
	Europe	Master file	Time and attendance	Processing payroll				
Taxes	**Corporate**	Income taxes		Property taxes				
	Europe		Sales taxes	Property taxes				
Financial Reporting	**Corporate**	Planning, budgeting and reporting	General ledger maintenance	Consolidation and related entries	Accounting policies and procedures	Footnotes	Account analysis and reconciliation	Journal entry processing
	Europe	Planning, budgeting and reporting	General ledger maintenance		Accounting policies and procedures	Footnotes	Account analysis and reconciliation	Journal entry processing
Information Systems	**Corporate**	Change management	Physical and logical security	Operations				
	Europe	Change management	Physical and logical security	Operations				
Miscellaneous	**Corporate**	Restructuring and impairments	Acquisitions	Divestitures	Other assets	Other liabilities	Equity method investments	Miscellaneous income and expense
	Europe	Restructuring and impairments	Acquisitions	Divestitures	Other assets	Other liabilities		Miscellaneous income and expense

Appendix IV — Example of a Business Process/Cycle Risk Assessment

Following is an example of how to perform a business process/cycle risk assessment by sub-process/ sub-cycle:

1. Determine significant risk factors that should be evaluated for each sub-cycle.
2. Assess the risk level as high, medium, or low for each risk factor in each sub-cycle.
3. Assign an overall risk rating (high, medium, or low) for each sub-cycle based upon an average of the individual risk factors for that sub-cycle.

Below are examples of individual risk factors:

Impact on Financial Statements	Misstatement or lack of controls could result in material misstatement in financial reporting
Complexity of the Process	Complexity as a function of financial statement data compilation or technical knowledge involved in determination of financial statement amount
Volume of Transactions	Number of transactions in a given period
Centralization of the Process	Centralization and direct control of processes by upper management
Inherent Risk in the Process	Inherent risk of errors or irregularities due to fraud

The risk assessment is performed to prioritize the assessment of controls and maximize the effectiveness and efficiency of the Section 404 project. Higher-risk cycles would normally be subject to more robust testing of all relevant assertions for each significant account, whereas lower-risk cycles would normally be subject to reduced testing. For example, for lower-risk cycles, management may use the lower end of ranges for sample sizes when performing tests, or management may perform testing earlier in the fiscal year. With respect to evaluations of the risk for each factor, suggested interpretations of the three ratings (high, medium, and low) are as follows:

High	The possibility of misstatement is high, or the balance has a material impact on the financial statements.
Medium	The possibility for misstatements in the given areas of the financial statements is moderate, or the process is subject to an average degree of error.
Low	The process is straightforward, and a misstatement in this area would have a minimal impact on the financial statements.

Based upon the risk assessment for each risk factor, an overall priority level for a given sub-cycle can be assessed. Management can look to the overall priority level to tailor the extent of testing that will be required in management's assessment of the relevant assertions for that sub-cycle.

Below is an example of how this evaluation may be documented (Note that a similar analysis would be performed for at least each individually important location):

RISK ASSESSMENT - US

	Impact on Financial Statements	Complexity of process	Volume of transaction	Centralization of process	Inherent risk of process	Priority A = H, B = M, C = L
Revenue & Receivables						
Customer Master	Medium	Medium	Low	Medium	Medium	**B**
Product Pricing	High	Medium	Low	Medium	Medium	**B**
Maintenance Pricing	High	Medium	Low	Medium	Medium	**B**
Service Pricing	High	Medium	Low	Medium	Medium	**B**
Revenue Forecasting	High	High	Medium	High	High	**A**
Order Entry	High	Medium	Medium	Medium	High	**A**
Shipping	High	Medium	Medium	Low	Medium	**A**
Service Invoicing	High	High	Medium	Medium	Medium	**A**
License Invoicing	High	Medium	Medium	Medium	Medium	**A**
Maintenance Invoicing	High	Medium	Medium	Medium	Medium	**A**
Cash Receipt	High	Low	High	Medium	High	**A**
Customer Returns	Medium	Medium	Low	Medium	High	**A**
Credit and Collection	High	Medium	Medium	Medium	High	**A**
Revenue Recognition	High	High	High	Medium	High	**A**
Purchasing & Payables						
Vendor Maintenance	Low	Medium	Medium	High	High	**B**
Requisitions	High	Medium	High	High	High	**A**
Purchase Orders	High	Medium	High	High	High	**A**
Goods Receipting	Medium	Low	Medium	High	Medium	**B**
Invoice Processing	High	Low	High	High	Medium	**B**
Cash Disbursements	High	Low	High	High	High	**A**
Treasury						
Cash Management	High	Low	High	High	High	**B**
Investment Management	High	Low	Low	Low	High	**C**
Derivatives	Low	High	Low	Low	High	**B**
Foreign Exchange	Low	High	High	High	Medium	**A**
Asset Management						
Fixed Asset Additions	Low	Low	Low	Medium	Low	**C**
Fixed Asset Transfers	Low	Low	Low	Medium	Low	**C**
Fixed Asset Retirements	Low	Low	Low	Medium	Low	**C**
Depreciation	Low	Low	Low	Medium	Low	**C**
Restructuring Reserves	Medium	Medium	Low	Low	High	**B**
Physical Maintenance	Low	Low	Low	Medium	Medium	**C**
Capital Leases	Medium	Medium	Low	High	High	**B**
Asset Disposal	Low	Low	Low	Medium	Medium	**C**

RISK Assessment - US	Impact on Financial Statements	Complexity of process	Volume of transaction	Centralization of process	Inherent risk of process	Priority A = H, B = M, C = L
Payroll and Human Resources						
New Employee	Low	Low	Low	High	Medium	**C**
Change In Status	Low	Low	Low	High	Low	**C**
Compensation	High	Medium	High	High	Low	**B**
Payroll Calculation	Medium	Low	High	High	Medium	**C**
Payroll Disbursement	Medium	Low	High	High	Medium	**C**
Payroll Accounting	Medium	Medium	Medium	High	Medium	**B**
Benefits Administration	Low	Medium	Medium	High	Medium	**C**
Taxes						
Net Operating Loss Monitoring	Low	High	Low	Medium	High	**B**
Disclosures	Low	Medium	Low	Low	Medium	**C**
Sales and Payroll	Medium	Medium	High	High	Medium	**A**
International Issues	Medium	High	Low	Low	High	**A**
Equity & Stock Administration						
Common Stock Activity	Low	Low	Low	Low	Low	**C**
Stock Option Activity	Low	Medium	Medium	Low	Low	**B**
Stock Purchase Plan	Low	Medium	Medium	Low	Low	**B**
Financial Reporting	High	High	High	Low	High	**A**
General Ledger Accounting						
Journal Entry Processing	High	Low	High	High	Medium	**B**
Period Closing	High	Medium	Low	High	Medium	**B**
Consolidation	High	High	Low	High	Medium	**A**
Management Estimates	Medium	High	Medium	Medium	High	**A**
Intercompany Transactions	Medium	Medium	Low	High	Medium	**B**
Adjusting Entries	Medium	High	Low	Medium	High	**A**
Financial Reporting						
Financial Reporting	High	High	Low	Medium	High	**A**
Related Parties	Low	Medium	Low	Medium	High	**A**
Segment Reporting	Medium	Medium	Low	Medium	Medium	**B**
Subsequent Events	Low	Medium	Low	Medium	Medium	**B**
Financial Statement Translation	Medium	High	Low	High	High	**A**
Preparation of Disclosures	Medium	High	Low	Low	High	**A**
Information Systems						
Control Environment	High	High	High	Medium	High	**A**
Program Development	High	High	High	Medium	High	**A**
Program Changes	None	High	High	High	High	**A**
Access to Programs and Data (Security)	None	High	Low	Low	Low	**C**
Computer Operations	None	High	High	Medium	High	**A**

RISK Assessment - US	Impact on Financial Statements	Complexity of process	Volume of transaction	Centralization of process	Inherent risk of process	Priority A = H, B = M, C = L
Mergers & Acquisitions						
Equity Investments	High	High	Low	Low	High	**A**
Acquisitions	High	High	Low	Low	High	**A**
Divestitures	High	High	Low	Low	High	**A**
Restructuring	High	High	Medium	High	High	**A**
Impairment	High	High	Medium	Low	High	**A**
Legal						
Litigation	Low	High	Low	Medium	High	**B**
Fraud Programs	Medium	High	Low	High	High	**A**
Commitments and Contingencies	Medium	Low	Low	Medium	Low	**B**

Appendix V — Flowchart Guidance and Sample

Guidelines for the preparation of flowcharts:

- **Structure of flowcharts:** Consistently following a standard layout for flowcharts ensures that each flowchart is logically structured and can be easily followed and understood. The following rules should be used to prepare flowcharts:
  - Keep the main flow of activities and controls in a vertical line down the middle of the flowchart.
  - To the left and right of the flowchart, add the main input and output documents and computer files.
  - The sequence of activities should flow from top to bottom.
  - Each flowchart should take up no more than one printed page. If a flowchart is larger than one page, activities should be grouped into higher-level processes and documented in separate flowcharts.
- **Content of flowcharts:** The detailed operations and controls that are associated with a company's various business processes can be documented in flowcharts, with each main activity in a given process being assigned its own chart. Given the amount of information contained within a series of flowcharts, it is important to make each flowchart easily understandable. Documentation at each level should contain a meaningful amount of information without providing too much data. For example:

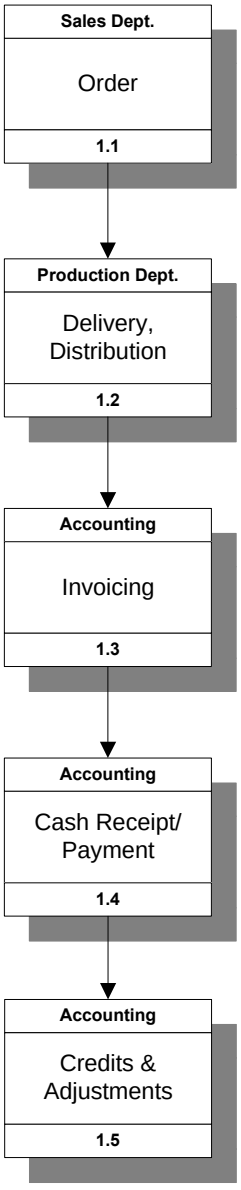
  Level 1: Overview of the process containing each of the main activities

  Level 2: Breakdown of the main activities into sub-activities

  Level 3: More detailed description of the sub-activities
- **Common problems to avoid:**
  - *A set of flowcharts that describes every process in detail:* These charts become very difficult to read because there is little information on the higher levels.
  - *A highly complex single-level flowchart:* A flowchart of this sort may be difficult for the reader to understand.

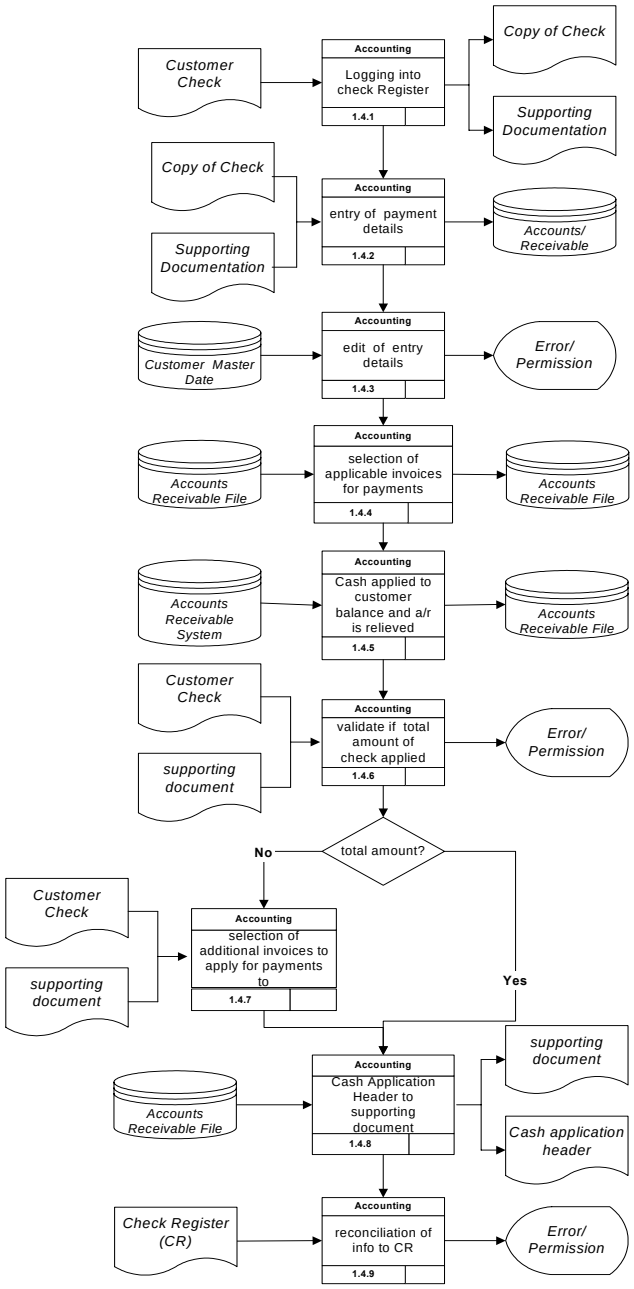
The following flowcharts provide an executive-level overview of the revenue process and the cash application sub-process. In some cases, companies may present more detailed flowcharts for the key sub-processes (i.e., Level 3).

Example of a Level 1 Flowchart: Sales Business Process

Process Flow & Controls Map	Description
	**1.1 Creation of sales order:** The creation of sales orders is initiated by a customer's order. The order management functions receive the order and enter all order data into the Sales and Accounts Receivable (SAR) system to create a sales order. The Sales Department creates the sales order in SAR by using a special item category in the sales order that automatically generates a delivery note. **1.2 Delivery and Distribution:** Goods are picked for distribution within the production department and dispatched to the customer with the delivery note. **1.3 Invoicing:** Based on the completed delivery and related delivery note, billing to the customer takes place. **1.4 Cash Receipt:** The cash application process includes both manual and automated procedures. Cash received into the lockbox(s) is automatically applied to customer accounts via a Cash Receipts file that is created by the Bank and sent to the mainframe computer system each night. **1.5 Credits and Adjustments:** Any required adjustments are made to customer accounts for returns, discounts, and other credits after required authorizations and supporting document are obtained.

Example of a Level 2 Flowchart: Cash Application Sub-process Showing Transactions and Controls

Process Flow & Controls Map



Description

1.4.1 The checks are forwarded to the Accounting Supervisor who logs them in a Check Register. The information recorded includes date of check, check number, check amount, customer name/number, and invoices that payment relates to. The Accounting Supervisor makes copies of the checks and sends the check copies along with the invoice hard copy supporting documentation to the Cash Application Department.

1.4.2 A representative of the Cash Application Department (representative) enters the customer number into the Cash Application screen within the Accounts Receivable system. The system validates the customer number against the Customer Master (Standing Data) file within the system.

1.4.3 If the system does not find the number, an error message is displayed indicating the number is invalid. The representative has the option of entering the customer last name and first name into a search screen to locate the customer number. If the system locates the customer master record for the customer number entered, a list of open invoices is generated on to the screen.

1.4.4 The next screen is for the first invoice number selected to apply payment to.

1.4.5 The representative is prompted to enter the amount of payment being applied to the invoice on a field at the top of the screen. The amount will typically match the total invoice amount (listed on the bottom of the screen), but there are times that only partial payment is applied to a particular invoice.

1.4.6 The invoice amount entered must be numeric and cannot be for an amount greater than the amount left to apply from the payment.

The representative scrolls through each invoice and applies cash to each applicable one. The system keeps a running total of the total amount of payment (per the check) and the amount left to be applied.

1.4.7 The representative cannot close out of the Cash Application screen without applying the total check amount to the open invoices.

1.4.8 The representative is responsible for printing out the Cash Application Header screen showing the high-level details of the cash application payment including check number, check amount, and check date. The representative staples the Cash Application Header screen printout to the check copy and supporting documentation. This information is forwarded back to the Accounting Supervisor at the end of the day.

1.4.9 The Accounting Supervisor reconciles the documentation back to the Check Register to ensure all checks were applied.

Appendix VI — Sample Control Matrix

Sub-Process	Control Objective	Description and Frequency of Control Activity	Financial Statement Area (1)	Information Processing Objectives (C,A,V, R) (2)	Assertions (CO, EO, RO, VA, PD) – (3)	P or D (4)	A or M (5)
Invoicing	Sales invoices are accurate.	The billing system receives shipped items from the shipping system and compares, line by line, the shipped items to the original order, making changes to the original order to reflect actual quantities shipped. (Multiple times a day)	Sales	C, A, V	CO, EO, VA	P	A
Invoicing	A sales invoice is generated for every shipment or work order.	Before an invoice is processed, shipment information is matched to customer-order information to ensure the information's accuracy and validity. (Multiple times a day)	Sales	A,V	A,C,E/O	P	A
G/L Posting	Sales are recorded in the proper period.	Management monitors sales and margins to ensure that they are aligned with expectations. (Monthly)	Sales	C, A, V	C,E/O	D	M
G/L Posting	Sales are recorded in the proper period. Postings that are made to cost of sales and/or inventory in the general ledger are appropriate.	The finance department reconciles sales in the general ledger with shipments on a weekly basis and follows up any reconciling items. This reconciliation is signed and filed. (Weekly)	Sales	C, A, V	C,E/O	D	M

1. Financial-statement area (F/S area)
2. Completeness (C), accuracy (A), validity (V), and restricted access (R)
3. Completeness (CO); existence or occurrence (EO); rights and obligations (RO); valuation or allocation (VA); and presentation and disclosure (PD)
4. Preventive (P) or detective (D) control
5. Automated (A) or manual (M) control

Appendix VII — Examples in Applying the Definitions of Significant Deficiency and Material Weakness

Source
The following examples of how to evaluate the significance of internal control deficiencies in various situations were taken **directly** from Appendix D of the Standard. These examples are for illustrative purposes only. Although the examples refer to the auditor, we believe they are equally applicable to management in its evaluation of the significance of internal control deficiencies.

Example VII-1.1 – Reconciliations of Intercompany Accounts Are Not Performed on a Timely Basis

Scenario A – Significant Deficiency

The company processes a significant number of routine intercompany transactions on a monthly basis. Individual intercompany transactions are not material and primarily relate to balance-sheet activity (for example, cash transfers between business units to finance normal operations). A formal management policy requires monthly reconciliation of intercompany accounts and confirmation of balances between business units. However, there is not a process in place to ensure that these procedures are performed. As a result, detailed reconciliations of intercompany accounts are not performed on a timely basis. Management does perform monthly procedures to investigate selected large-dollar differences between intercompany accounts. In addition, management prepares a detailed monthly variance analysis of operating expenses to assess their reasonableness.

Drawing only on these facts, the auditor should determine that this deficiency (i.e., the company's failure to reconcile intercompany accounts on a timely basis) represents a significant deficiency for the following reasons: It would be reasonable to expect that the magnitude of a financial-statement misstatement resulting from this deficiency would be more than inconsequential but less than material, because (1) individual intercompany transactions are not material and (2) the compensating controls (which operate monthly) should detect a material misstatement. Furthermore, the transactions are primarily restricted to balance-sheet accounts. However, the compensating detective controls are designed to detect material misstatements only. The controls do not address the detection of misstatements that are more than inconsequential but less than material. Thus there is a more-than-remote likelihood of a misstatement that is more than inconsequential but less than material.

Scenario B – Material Weakness

The company processes a significant number of intercompany transactions on a monthly basis. Intercompany transactions relate to a wide range of activities, including transfers of inventory with intercompany profit between business units, allocation of research and development costs to business units, and corporate charges. Individual intercompany transactions are frequently material. A formal management policy requires monthly reconciliation of intercompany accounts and confirmation of balances between business units. However, there is not a process in place to ensure that these procedures are performed on a consistent basis. As a result, reconciliations of intercompany accounts are not performed on a timely basis, and differences in intercompany accounts are frequent and significant. Management does not perform any alternative controls to investigate significant differences between intercompany accounts.

Using only these facts, the auditor should determine that this deficiency represents a material weakness for the following reasons: It is reasonable to expect that the magnitude of a financial-statement misstatement resulting from this deficiency would be material, because individual intercompany transactions are frequently material and relate to a wide range of activities. Additionally, actual unreconciled differences in intercompany accounts have been, and are, material. The likelihood of such a misstatement is more than remote because such misstatements have frequently occurred and compensating controls are not effective, either because they are not properly designed or they are not operating effectively. Taken together, the likelihood and potential magnitude of a financial-statement misstatement resulting from this internal-control deficiency meet the definition of a material weakness.

Example VII-1.2 – Modifications in the Terms of a Standard Sales Contract Not Reviewed to Evaluate Impact on Timing and Amount of Revenue Recognition

Scenario A – Significant Deficiency

The company uses a standard sales contract for most transactions. Individual sales transactions are not material to the entity. Sales personnel are allowed to modify the terms of sales contracts. The company's accounting function reviews significant or unusual modifications in the terms of sales contracts but does not review changes in the standard shipping terms. The changes in the standard shipping terms could delay the timing of revenue recognition. Management reviews gross margins on a monthly basis and investigates any significant or unusual relationships. In addition, management reviews the reasonableness of inventory levels at the end of each accounting period. The entity has experienced limited situations in which revenue has been inappropriately recorded before shipment, but amounts have not been material.

Using only these facts, the auditor should determine that this deficiency represents a significant deficiency for the following reasons: It is reasonable to expect that the magnitude of a financial-statement misstatement resulting from this deficiency would be more than inconsequential but less than material, because individual sales transactions are not material and the compensating detective controls (which operate monthly and at the end of each financial-reporting period) should reduce the likelihood that a material misstatement will go undetected. Furthermore, the risk of a material misstatement is limited to revenue-recognition errors related to shipping terms and does not lie with broader sources of error in revenue recognition. However, the compensating detective controls are designed to detect material misstatements only. The controls do not effectively address the detection of misstatements that are more than inconsequential but less than material, as evidenced by situations in which transactions that were not material were improperly recorded. Thus there is a more-than-remote likelihood of a misstatement that is more than inconsequential but less than material.

Scenario B – Material Weakness

The company has a standard sales contract, but sales personnel frequently modify the terms of the contract. The nature of the modifications can affect the timing and amount of revenue that the company recognizes. Individual sales transactions are frequently material to the entity, and the gross margin can vary significantly for each transaction. The accounting function does not regularly review modifications in the terms of sales contracts. Although management reviews gross margins on a monthly basis, the significant differences in gross margins for individual transactions make it difficult for management to detect potential misstatements. Improper revenue recognition has occurred, and the amounts have been material.

Drawing only on these facts, the auditor should determine that this deficiency represents a material weakness for the following reasons: It would be reasonable to expect that the magnitude of a financial-statement misstatement resulting from this deficiency would be material, because individual sales transactions are frequently material and gross margin can vary significantly with each transaction (which would make compensating detective controls based on a reasonableness review ineffective). Additionally, improper

revenue recognition has occurred, and the amounts have been material. Thus there is a more-than-remote likelihood of material misstatements. Taken together, the likelihood and potential magnitude of a financial-statement misstatement resulting from this internal-control deficiency meet the definition of a material weakness.

Scenario C – Material Weakness

The company has a standard sales contract, but sales personnel frequently modify the terms of the contract. Sales personnel often grant unauthorized and unrecorded sales discounts to customers without the knowledge of the accounting department. Customers deduct these amounts when they pay their invoices; meanwhile, the accounting department records those same amounts as outstanding balances on the accounts receivable sub-ledger. Although these amounts are individually insignificant, they are material in the aggregate and have occurred consistently over the past few years. From these facts alone, the auditor should determine that this deficiency represents a material weakness for the following reasons: It would be reasonable to expect that the magnitude of a financial-statement misstatement resulting from this deficiency would be material, because the frequency of the deficiency allows insignificant amounts to become material in the aggregate. The likelihood that a material financial-statement misstatement will result from this internal-control deficiency is more than remote (even assuming that the amounts were fully reserved for in the company's allowance for uncollectible accounts), because of the likelihood that the gross accounts-receivable balance will be materially misstated. Therefore, this internal-control deficiency meets the definition of a material weakness.

Example VII-1.3 – Identification of Several Deficiencies

Scenario A – Material Weakness

During its assessment of internal control over financial reporting, management detected the deficiencies listed below. Based on the context in which the deficiencies occur, management and the auditor agree that, individually, these deficiencies represent significant deficiencies:

- Inadequate segregation of duties pertaining to certain controls that govern access to the company’s information system
- Several instances of transactions that were not properly recorded in subsidiary ledgers (transactions were not material, either individually or in the aggregate)
- A lack of timely reconciliations of the account balances that were affected by the improperly recorded transactions

Looking at these facts only, the auditor should determine that the combination of these significant deficiencies represents a material weakness for the following reasons: The auditor ascertained that, individually, these deficiencies represent a more-than-remote likelihood of a misstatement that is more than inconsequential but less than material. However, each of these significant deficiencies affects the same set of accounts. Taken together, these significant deficiencies represent a more-than-remote likelihood that a material misstatement could not be prevented or detected. Therefore, in combination, these significant deficiencies represent a material weakness.

Scenario B – Material Weakness

During its assessment of internal control over financial reporting, management of a financial institution detects deficiencies in the design of controls for the estimation of credit losses (a critical accounting estimate); the operating effectiveness of controls for initiating, processing, and reviewing adjustments of the allowance for credit losses; and the operating effectiveness of controls designed to prevent and detect the improper

recognition of interest income. Management and the auditor agree that, in the overall context, each of these deficiencies represents a significant deficiency. During the past year, the company experienced significant growth in the loan balances that were subjected to the controls governing credit-loss estimation and revenue recognition, and further growth is expected in the upcoming year.

Analyzing only these facts, the auditor should determine that the combination of these significant deficiencies represents a material weakness for the following reasons:

- The balances of the loan accounts that are affected by these significant deficiencies have increased over the past year and are expected to increase in the future.
- This growth in loan balances, coupled with the combined effect of the significant deficiencies, results in a more-than-remote likelihood of a material misstatement of the allowance for credit losses or interest income.

Therefore, in combination, these deficiencies meet the definition of a material weakness.

Appendix VIII — SEC: Frequently Asked Questions

Source
The SEC staff's *Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports Frequently Asked Questions* is an exact reproduction of the pages included on the SEC's website.

Office of the Chief Accountant
Division of Corporation Finance:

Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports Frequently Asked Questions

The answers to these frequently asked questions represent the views of the staffs of the Office of the Chief Accountant and the Division of Corporation Finance. They are not rules, regulations or statements of the Securities and Exchange Commission. Further, the Commission has neither approved nor disapproved them.

Note: Since the adoption of the Commission's Rules on *Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports* (Release No. 34-47986, June 5, 2003), we have received questions regarding the implementation and interpretation of the rules. Questions on accounting matters related to management's report on internal control over financial reporting should be directed to Nancy Salisbury (salisburyn@sec.gov) or Esmeralda Rodriguez (rodrigueze@sec.gov) in the Office of the Chief Accountant, Mail Stop 1103, 450 Fifth Street, NW, Washington, DC 20549; telephone: (202) 942-4400. Other disclosure and filing questions should be directed to Sean Harrison at (202) 942-2910, or Jonathan Ingram at (202) 942-2900 in the Division of Corporation Finance.

Question 1

Q: Financial Accounting Standards Board (FASB) Interpretation No. 46 (revised December 2003), *Consolidation of Variable Interest Entities — An Interpretation of ARB No. 51*, requires that registrants apply that guidance and, if applicable, consolidate entities based on characteristics other than voting control no later than the period ending March 15, 2004, or December 15, 2004 for small business issuers. In instances where the registrant lacks the ability to dictate or modify the internal controls of an entity consolidated pursuant to Interpretation No. 46, it may not have legal or contractual rights or authority to assess the internal controls of the consolidated entity even though that entity's financial information is included in the registrant's financial statements. Similarly, for entities accounted for via proportionate consolidation in accordance with Emerging Issues Task Force Issue No. 00-1 (EITF 00-1), management may not have the ability to assess the internal controls. How should management's report on internal control over financial reporting address these situations?

> **A**: We would typically expect management's report on internal control over financial reporting to include controls at all consolidated entities, irrespective of the basis for consolidation. However, in a situation where the entity was in existence prior to December 15, 2003 and is consolidated by virtue of Interpretation No. 46 (i.e., would not have been consolidated in the absence of application of that guidance) and where the registrant does not have the right or authority to assess the internal controls of the consolidated entity and also lacks the ability, in practice, to make that assessment, we believe management's report on internal control over financial reporting should provide disclosure in

the body of its Form 10-K or 10-KSB regarding such entities. For example, a registrant could refer readers to a discussion of the scope of management's report on internal control over financial reporting in a section of the annual report entitled "Scope of Management's Report on Internal Control Over Financial Reporting." The registrant should disclose in the body of the Form 10-K or 10-KSB that it has not evaluated the internal controls of the entity and should also note that the registrant's conclusion regarding the effectiveness of its internal control over financial reporting does not extend to the internal controls of the entity. The registrant should also disclose any key sub-totals, such as total and net assets, revenues and net income that result from consolidation of entities whose internal controls have not been assessed. The disclosure should note that the financial statements include the accounts of certain entities consolidated pursuant to FIN 46 or accounted for via proportionate consolidation in accordance with EITF 00-1 but that management has been unable to assess the effectiveness of internal control at those entities due to the fact that the registrant does not have the ability to dictate or modify the controls of the entities and does not have the ability, in practice, to assess those controls.

Question 2

Q: Is a registrant required to evaluate the internal control over financial reporting of an equity method investment?

A: The accounts of an equity method investee are not consolidated on a line-by-line basis in the financial statements of the investor, and as such, controls over the recording of transactions into the investee's accounts are not part of the registrant's internal control structure. However, the registrant must have controls over the recording of amounts related to its investment that are recorded in the consolidated financial statements. Accordingly, a registrant would have to consider, among other things, the controls over: the selection of accounting methods for its investments, the recognition of equity method earnings and losses, its investment account balance, etc. For example, a registrant might require that, at least annually, its equity method investees provide audited financial statements as a control over the recognition of equity method earnings and losses. However, nothing precludes a registrant from evaluating the control over financial reporting of an equity method investment, and there may be circumstances where it is not only appropriate but also may be the most effective form of evaluation. For purposes of applying this guidance, we make no distinction between those equity method investments for which the registrant is required to file audited financial statements pursuant to Rule 3-09 of Regulation S-X and those where no such requirement is triggered.

Question 3

Q: If a registrant consummates a material purchase business combination during its fiscal year, must the internal control over financial reporting of the acquired business be included in management's report on internal control over financial reporting for that fiscal year?

A: As discussed above, we would typically expect management's report on internal control over financial reporting to include controls at all consolidated

entities. However, we acknowledge that it might not always be possible to conduct an assessment of an acquired business's internal control over financial reporting in the period between the consummation date and the date of management's assessment. In such instances, we would not object to management referring in the report to a discussion in the registrant's Form 10-K or 10-KSB regarding the scope of the assessment and to such disclosure noting that management excluded the acquired business from management's report on internal control over financial reporting. If such a reference is made, however, management must identify the acquired business excluded and indicate the significance of the acquired business to the registrant's consolidated financial statements. Notwithstanding management's exclusion of an acquired business's internal controls from its annual assessment, a registrant must disclose any material change to its internal control over financial reporting due to the acquisition pursuant to Exchange Act Rule 13a-15(d) or 15d-15(d), whichever applies. In addition, the period in which management may omit an assessment of an acquired business's internal control over financial reporting from its assessment of the registrant's internal control may not extend beyond one year from the date of acquisition, nor may such assessment be omitted from more than one annual management report on internal control over financial reporting.

Question 4

Q: If management, the accountant, or both conclude in a report included in a timely filed Form 10-K or 10-KSB that the registrant's internal control over financial reporting is not effective, would the registrant still be considered timely and current for purposes of Rule 144 and Forms S-2, S-3, and S-8 eligibility?

A: Yes, as long as the registrant's other reporting obligations are timely satisfied. As has previously been the case, the auditor's report on the audit of the financial statements must be unqualified.

Question 5

Q: May management qualify its conclusions by saying that the registrant's internal control over financial reporting are effective subject to certain qualifications or exceptions or express similar positions?

A: No. Management may not state that the registrant's controls and procedures are effective except to the extent that certain problems have been identified or express similar qualified conclusions. Rather, management must take those problems into account when concluding whether the registrant's internal control over financial reporting is effective. Management may state that controls are ineffective for specific reasons. In addition, management may not conclude that the registrant's internal control over financial reporting is effective if a material weakness exists in the registrant's internal control over financial reporting.

Question 6

Q: If management's report on internal control over financial reporting does not identify a material weakness but the accountant's attestation report does, or vice versa, does this constitute a disagreement between the registrant and the auditor that must be reported pursuant to Item 304 of Regulation S-K or S-B?

A: No, unless the situation results in a change in auditor that would require disclosure under Item 304 of Regulation S-K or S-B. However, such differences in identification of material weaknesses could trigger other disclosure obligations.

Question 7

Q: When should a registrant determine whether it is an accelerated filer for purposes of determining when it must comply with Items 308(a) and (b) of Regulations S-K and S-B?

A: As provided in Exchange Act Rule 12b-2, a registrant that is not already subject to accelerated filing should determine whether it is an accelerated filer at the end of its fiscal year, based on the market value of its public float of its common equity as of the last business day of its most recently completed second fiscal quarter. Consideration should also be given to the other components of the Rule 12b-2 definition (i.e. the registrant has been subject to Exchange Act reporting for at least 12 months, has filed at least one annual report, and is not eligible to use Forms 10-KSB and 10-QSB).

Question 8

Q: Is a registrant required to provide management's report on internal control over financial reporting, and the related auditor attestation report, when filing a transition report on Form 10-K or 10-KSB?

A: Yes. Because transition reports filed on Forms 10-K or 10-KSB (whether by rule or by election) must contain audited financial statements, they must also include management's report on internal control, subject to the transition provisions specified in Release No. 34-47986. The transition provisions relating to management's report on internal control should be applied to the *transition period as if it were a fiscal year*. Transition reports on Form 10-Q or 10-QSB are not required to include a management report on internal control.

Question 9

Q: Is a registrant required to disclose changes or improvements to controls made as a result of preparing for the registrant's first management report on internal control over financial reporting?

A: Generally we expect a registrant to make periodic improvements to internal controls and would welcome disclosure of all material changes to controls, whether or not made in advance of the compliance date of the rules under Section 404 of the Sarbanes-Oxley Act. However, we would not object if a registrant did not disclose changes made in preparation for the registrant's first management report on internal control over financial reporting. However, if the registrant were to identify a material weakness, it should carefully consider whether that fact should be disclosed, as well as changes made in response to the material weakness.

After the registrant's first management report on internal control over financial reporting, pursuant to Item 308 of Regulations S-K or S-B, the registrant is required to identify and disclose any material changes in the registrant's internal control over financial reporting in each quarterly and annual report. This would encompass disclosing a change (including an improvement) to internal control over financial reporting that was not necessarily in response to an identified significant deficiency or material weakness (i.e. the implementation of a new information system) if it materially affected the registrant's internal control over financial reporting. Materiality, as with all materiality judgments in this area, would be determined upon the basis of the impact on internal control over financial reporting and the materiality standard articulated in TSC Industries, Inc. v. Northway, Inc. 426 U.S. 438 (1976) and Basic Inc. v. Levinson, 485 U.S. 224 (1988). This would also include disclosing a change to internal control over financial reporting related to a business combination for which the acquired entity that has been or will be excluded from an annual management report on internal control over financial reporting as contemplated in Question 3 above. As an alternative to ongoing disclosure for such changes in internal control over financial reporting, a registrant may choose to disclose all such changes to internal control over financial reporting in the annual report in which its assessment that encompasses the acquired business is included.

Question 10

Q: The definition of the term "internal control over financial reporting" does not encompass a registrant's compliance with applicable laws and regulations, with the exception of compliance with the applicable laws and regulations directly related to the preparation of financial statements, such as the Commission's financial reporting requirements. Are all aspects of the rules promulgated under the Sarbanes-Oxley Act, for example, within that definition?

> **A**: No. While, it may be possible to connect the violation of any law, rule or regulation to the financial statements by observing that if the violation is significant enough it will have a material impact on the registrant's financial statements, we do not believe that compliance with all laws fits within the definition. The Commission's financial reporting requirements and the Internal Revenue Code are examples of regulations that are directly related to the preparation of the financial statements. Conversely, rules requiring disclosure as to the existence of a code of ethics or disclosure as to the existence of an audit committee financial expert are examples of rules promulgated under the Sarbanes-Oxley Act that are not directly related to the preparation of financial statements.
>
> However, as part of management's evaluation of a registrant's disclosure controls and procedures, management must appropriately consider the registrant's compliance with other laws, rules and regulations. Such consideration should include assessing whether the registrant (1) adequately monitors such compliance, and (2) has appropriate disclosure controls and procedures to ensure that required disclosure of legal or regulatory matters is provided. Evaluation of disclosure controls and procedures and internal control over financial reporting in respect of compliance with applicable laws or regulations does intersect at certain points, including, for example, whether the registrant has controls to ensure that the effects of non-compliance with laws, rules and regulations are recorded in the registrant's financial statements,

including the recognition of probable losses under FASB Statement No. 5, *Accounting for Contingencies.*

Question 11

Q: Must identified significant deficiencies be disclosed either as part of management's report on internal control over financial reporting or elsewhere in a registrant's periodic reports?

A: A registrant is obligated to identify and publicly disclose all material weaknesses. If management identifies a significant deficiency it is not obligated by virtue of that fact to publicly disclose the existence or nature of the significant deficiency. However, if management identifies a significant deficiency that, when combined with other significant deficiencies, is determined to be a material weakness, management must disclose the material weakness and, to the extent material to an understanding of the disclosure, the nature of the significant deficiencies. In addition, if a material change is made to either disclosure controls and procedures or to internal control over financial reporting in response to a significant deficiency, the registrant is required to disclose such change and should consider whether it is necessary to discuss further the nature of the significant deficiency in order to render the disclosure not misleading. A registrant's auditor that is aware of a significant deficiency is required to communicate the significant deficiency to the audit committee as required by PCAOB Auditing Standard No. 2.

Question 12

Q: Many registrants with global operations have a lag in reporting the financial results of certain foreign subsidiaries for financial reporting purposes. For example, a registrant with a December 31 year-end may consolidate the operations of certain foreign subsidiaries with a November 30 year-end. Is this difference in period ends also acceptable in relation to the assessment of internal control over financial reporting?

A: Yes.

Question 13

Q: The Commission's adopting release for its rules pursuant to Section 404 of the Sarbanes-Oxley Act (Release No. 34-47986) provides that the terms "significant deficiency" and "material weakness" have the same meaning for purposes of those rules as they do under generally accepted auditing standards and attestation standards. PCAOB Auditing Standard No. 2 modified the definitions of the terms "significant deficiency" and "material weakness." Does the Commission staff intend to look to the definitions as they existed when the adopting release was issued or as they have been revised by the PCAOB?

A: When the Commission published its adopting release, the Commission expressed an intention to incorporate the definitions of "significant deficiency" and "material weakness" as they exist in the standards used by auditors of public companies. Looking to the definitions as revised by the PCAOB is

consistent with this intention and, accordingly, the SEC staff will apply the PCAOB definitions in interpreting the Commission rules in this area.

Question 14

Q: In many situations, a registrant relies on a third party service provider to perform certain functions where the outsourced activity affects the initiation, authorization, recording, processing or reporting of transactions in the registrant's financial statements, such as payroll. In assessing internal controls over financial reporting, management may rely on a Type 2 SAS 70 report performed by the auditors of the third party service providers. If the auditors of the third party service provider are the same as the auditors of the registrant, may management still rely on that report? Additionally, may management rely on a Type 2 SAS 70 report on the third party based on a different year-end?

A: In situations where management has outsourced certain functions to third party service provider(s), management maintains a responsibility to assess the controls over the outsourced operations. However, management would be able to rely on the Type 2 SAS 70 report even if the auditors for both companies were the same. On the other hand, if management were to engage the registrant's audit firm to also prepare the Type 2 SAS 70 report on the service organization, management would not be able to rely on that report for purposes of assessing internal control over financial reporting. Management would be able to rely on a Type 2 SAS 70 report on the service provider that is as of a different year-end. Note, however, that management is still responsible for maintaining and evaluating, as appropriate, controls over the flow of information to and from the service organization.

Question 15

Q: What is the impact of combining the auditor's attestation report on management's assessment of internal controls over financial reporting with the audit report on the financial statements?

A: Item 2-02 of Regulation S-X permits the auditor to combine the attestation report on management's assessment on internal control with the auditor's report on the financial statements. However, in determining whether to combine the reports, the auditor should take into account any issues that may arise if its audit report on the financial statements is expected to be reissued or incorporated by reference into a filing under the Securities Act.

Question 16

Q: Will the SEC be providing guidance on specific considerations relating to internal control over financial reporting for small business issuers?

A: Although the Commission's final rule implementing Section 404 of the Act does not distinguish between large and small issuers, the Commission, as noted in the release accompanying the final rule, recognized that many smaller issuers might encounter difficulties in evaluating their internal control over financial

reporting. The SEC staff would support efforts by bodies such as COSO to develop an internal control framework specifically for smaller issuers.

Question 17

Q: To what extent may management rely on the registrant's auditor to assist in its development of an assessment process and documentation process in preparation of issuing management's report on internal control over financial reporting?

A: The auditor is allowed to provide limited assistance to management in documenting internal controls and making recommendations for changes to internal controls. However, management has the ultimate responsibility for the assessment, documentation and testing of the registrant's internal controls over financial reporting.

Question 18

Q: What sources of guidance are available to management to assist them in fulfilling their responsibilities regarding management's assessment and documentation of the internal control over financial reporting?

A: Several sources of guidance are available on the topic of management's assessment of internal control including, for example: the existing books and records requirements; the Commission's final rule on Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports (Release No. 34-47986); and, as referenced in the release on the final rule, the reports published by the Committee of Sponsoring Organizations of the Treadway Commission on internal control.

Appendix IX — PCAOB: Frequently Asked Questions

Source
The PCAOB staff's *Questions and Answers: Auditing Internal Control Over Financial Reporting* is an exact reproduction of the pages included on the PCAOB's website.

PCAOB
Public Company Accounting Oversight Board

1666 K Street, N.W.
Washington, DC 20006
Telephone: (202) 207-9100
Facsimile: (202) 862-8430
www.pcaobus.org

STAFF QUESTIONS AND ANSWERS

AUDITING INTERNAL CONTROL OVER FINANCIAL REPORTING

JUNE 23, 2004

Summary: Staff questions and answers set forth the staff's opinions on issues related to the implementation of the standards of the Public Company Accounting Oversight Board ("PCAOB" or "Board"). The staff publishes questions and answers to help auditors implement, and the Board's staff administer, the Board's standards. The statements contained in the staff questions and answers are not rules of the Board, nor have they been approved by the Board.

The following staff questions and answers related to PCAOB Auditing Standard No. 2, *An Audit of Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements* ("Auditing Standard No. 2"), were prepared by the Office of the Chief Auditor. Questions should be directed to Laura Phillips, Associate Chief Auditor (202/207-9111; phillipsl@pcaobus.org) or Greg Fletcher, Assistant Chief Auditor (202/207-9203; fletcherg@pcaobus.org).

* * *

General

Q1. What is the authoritative status of the Background and Basis for Conclusions appendix in a Board's standard?

A1. All appendices of auditing standards issued by the Board, including the Background and Basis for Conclusions, are an integral part of the standard and carry the same authoritative weight as the body of the standard.

STAFF QUESTIONS & ANSWERS

Q2. What is the authoritative status of the Notes included within the body of a Board's standard?

> **A2.** Both the Notes and footnotes to a Board standard are an integral part of the standard and carry the same authoritative weight as any other information in the body of, or appendices to, the standard.

Independence

Q3. Paragraph 33 of Auditing Standard No. 2 states: "The auditor must not accept an engagement to provide internal control-related services to an issuer for which the auditor also audits the financial statements unless that engagement has been specifically pre-approved by the audit committee." Although the word "non-audit" does not appear in that requirement, do only non-audit internal control-related services need to be specifically pre-approved?

> **A3.** The pre-approval requirement in Auditing Standard No. 2 applies to *any* internal control-related services, regardless of whether they are classified as audit or non-audit services for proxy disclosure purposes or otherwise. Every proposed engagement by the issuer's auditor to provide internal control-related services merits specific attention by the audit committee so that the audit committee can determine whether the performance of the services would impair the auditor's independence and whether management's involvement in the services is substantive and extensive.

Q4. Under Auditing Standard No. 2, an auditor cannot accept an engagement to provide internal control-related services unless the audit committee has evaluated the actual, individual control-related service before the auditor was engaged. An auditor might have been engaged by an issuer to perform internal control-related services prior to the effective date of Auditing Standard No. 2, at which time those services were pre-approved in a manner that would not satisfy the requirement in Auditing Standard No. 2. Further, those services might be ongoing such that the auditor continues to provide internal control-related services *after* the effective date of Auditing Standard No. 2 that were pre-approved *prior* to the effective date of Auditing Standard No. 2 in a manner that does not satisfy the auditor's requirement in Auditing Standard No. 2. Is there any

STAFF QUESTIONS & ANSWERS

grandfathering for these types of engagements in which their original pre-approval would be considered sufficient under Auditing Standard No. 2?

> **A4.** No, there is no grandfathering for internal control-related engagements that were pre-approved prior to the effective date of Auditing Standard No. 2 in a manner that would not satisfy the requirement in Auditing Standard No. 2 if the provision of services is ongoing after the effective date of the standard. If the auditor has been engaged to perform internal control-related services that were pre-approved prior to the effective date of Auditing Standard No. 2 in a manner that does not satisfy the requirements of Auditing Standard No. 2 and if those services are ongoing after the effective date of Auditing Standard No. 2, the auditor should request the audit committee to specifically evaluate the independence implications of the continuation of those services as soon as practicable. This type of remedial involvement of the audit committee is consistent with the emphasis and vigilance that is appropriate for the audit committee to have regarding approval of internal control-related services.

Scope and Extent of Testing

Q5. Several passages in Auditing Standard No. 2 refer to "financial statements and related disclosures." Do these references to "related disclosures" extend the auditor's evaluation and testing of controls to controls over the preparation of management's discussion and analysis ("MD&A")?

> **A5.** No. References in Auditing Standard No. 2 to "financial statements and related disclosures" refer to a company's financial statements and notes as presented in accordance with generally accepted accounting principles ("GAAP"). These references do not extend to the preparation of MD&A or other similar financial information presented outside a company's GAAP-basis financial statements and notes.

Q6. If management implements, late in the year, a new accounting system that significantly affects the processing of transactions for significant accounts, and if the majority of the year's transactions were processed on the old system, does the auditor need to test controls over the *new* system? Given the same scenario, does the auditor need to test controls over the *old* system?

STAFF QUESTIONS & ANSWERS

A6. To audit internal control over financial reporting, the auditor will need to test controls over the new system. Paragraphs 147-149 of Auditing Standard No. 2 provide relevant directions to the auditor in this situation. Those paragraphs state that the auditor's opinion on whether management's assessment of the effectiveness of internal control over financial reporting is fairly stated relates to the effectiveness of the company's internal control over financial reporting as of a *point in time*. Furthermore, Section 404(a) of the Act requires that this assessment be as of the end of the issuer's most recent fiscal year. Because controls over the *new* system, which significantly affect the processing of transactions for significant accounts, are the controls that are operating as of the date of management's assessment, the auditor should test controls over the new system.

Although the auditor would not be required to test controls over the *old* system to have sufficient evidence to support his or her opinion on management's assessment of the effectiveness of internal control over financial reporting as of the end of the issuer's fiscal year, the old system is relevant to the audit of the financial statements. In the audit of the financial statements, the auditor should have an understanding of the internal control over financial reporting, which includes the old system. Additionally, to assess control risk for specific financial statement assertions at less than the maximum, the auditor is required to obtain evidence that the relevant controls operated effectively during the *entire period* upon which the auditor plans to place reliance on those controls. Paragraphs 150 and 151 of Auditing Standard No. 2 provide relevant directions to the auditor in this situation.

Q7. Paragraph 140 of Auditing Standard No. 2 includes the following circumstance as a significant deficiency and a strong indicator of a material weakness:

> Identification by the auditor of a material misstatement in financial statements in the current period that was not initially identified by the company's internal control over financial reporting. (This is a strong indicator of a material weakness even if management subsequently corrects the misstatement.)

Historically, many auditors have worked with companies closely at year-end, performing auditing procedures on preliminary drafts of the financial statements and providing

STAFF QUESTIONS & ANSWERS

feedback over a period of time on each successive draft. If the auditor identifies a misstatement in a preliminary draft of financial statements, does this represent a significant deficiency and a strong indicator of a material weakness? Do discussions between management and the auditor regarding the adoption of a new accounting principle or an emerging issue that have, in the past, been seen as a normal part of a high quality audit, need to be postponed until after the company has completed its related accounting?

A7. The inclusion of this circumstance in Auditing Standard No. 2 as a significant deficiency and a strong indicator of a material weakness emphasizes that a company must have effective internal control over financial reporting on its own. More specifically, the results of auditing procedures cannot be considered when evaluating whether the company's internal control provides reasonable assurance that the company's financial statements will be presented fairly in accordance with generally accepted accounting principles. There are a variety of ways that a company can emphasize that it, rather than the auditor, is responsible for the financial statements and that the company has effective controls surrounding the preparation of financial statements.

Modifying the traditional audit process such that the company provides the auditor with only a single draft of the financial statements to audit when the company believes that all its controls over the preparation of the financial statements have fully operated is one way to demonstrate management's responsibility and to be clear that all the company's controls have operated. However, this process is not necessarily what was expected to result from the implementation of Auditing Standard No. 2. Such a process might make it difficult for some companies to meet the accelerated filing deadlines for their annual reports. More importantly, such a process, combined with the accelerated filing deadlines, might put the auditor under significant pressure to complete the audit of the financial statements in too short a time period thereby impairing, rather than improving, audit quality. Therefore, some type of information-sharing on a timely basis between management and the auditor is necessary.

A company may share interim drafts of the financial statements with the auditor. The company can minimize the risk that the auditor would determine that his or her involvement in this process might represent a significant deficiency or

STAFF QUESTIONS & ANSWERS

material weakness through clear communications (either written or oral) with the auditor about the following:

- state of completion of the financial statements;
- extent of controls that had operated or not operated at the time; and
- purpose for which the company was giving the draft financial statements to the auditor.

For example, a company might give the auditor draft financial statements to audit that lack two notes required by generally accepted accounting principles. Absent any communication from the company to clearly indicate that the company recognizes that two specific required notes are lacking, the auditor might determine that the lack of those notes constitutes a material misstatement of the financial statements that represents a significant deficiency and is a strong indicator of a material weakness. On the other hand, if the company makes it clear when it provides the draft financial statements to the auditor that two specific required notes are lacking and that those completed notes will be provided at a later time, the auditor would not consider their omission at that time a material misstatement of the financial statements.

As another example, a company might release a partially completed note to the auditor and make clear that the company's process for preparing the numerical information included in a related table is complete and, therefore, that the company considers the numerical information to be fairly stated even though the company has not yet completed the text of the note. At the same time, the company might indicate that the auditor should not yet subject the entire note to audit, but only the table. In this case, the auditor would evaluate only the numerical information in the table and the company's process to complete the table. However, if the auditor identifies a misstatement of the information in the table, he or she should consider that circumstance a misstatement of the financial statements. If the auditor determines that the misstatement is material, a significant deficiency as well as a strong indicator of a material weakness would exist.

STAFF QUESTIONS & ANSWERS

This type of analysis, focusing on the company's responsibility for internal control, may be extended to other types of auditor involvement. For example, many audit firms prepare accounting disclosure checklists to assist both companies and auditors in evaluating whether financial statements include all the required disclosures under GAAP. Obtaining a blank accounting disclosure checklist from the company's auditor and independently completing the checklist as part of the procedures to prepare the financial statements is not, by itself, an indication of a weakness in the company's controls over the period-end financial reporting process. As another example, if the company obtains the blank accounting disclosure checklist from its auditor, requests the auditor to complete the checklist, and the auditor determines that a material required disclosure is missing, that situation would represent a significant deficiency and a strong indicator of a material weakness.

These evaluations, focusing on the company's responsibility for internal control over financial reporting, will necessarily involve judgment on the part of the auditor. A discussion with management about an emerging accounting issue that the auditor has recently become aware of, or the application of a complex and highly technical accounting pronouncement in the company's particular circumstances, are all types of timely auditor involvement that should not necessarily be indications of weaknesses in a company's internal control over financial reporting. However, as described above, clear communication between management and the auditor about the purpose for which the auditor is being involved is important. Although the auditor should not determine that the implications of Auditing Standard No. 2 force the auditor to become so far removed from the financial reporting process on a timely basis that audit quality is impaired, some aspects of the traditional audit process may need to be carefully structured as a result of this increased focus on the effectiveness of the company's internal control over financial reporting.

Q8. If an issuer decides to forego the required testing or documentation that would form a sufficient basis for management's assessment of the effectiveness of internal control over financial reporting, may the auditor simply render an adverse opinion on internal control over financial reporting? In this circumstance, could the auditor render an adverse opinion on management's assessment but render an unqualified opinion on the effectiveness of internal control over financial reporting?

STAFF QUESTIONS & ANSWERS

A8. No. Paragraph 20 of Auditing Standard No. 2 describes the responsibilities that management is required to fulfill for the auditor to satisfactorily complete an audit of internal control over financial reporting. These responsibilities include management evaluating the effectiveness of the company's internal control over financial reporting and supporting its evaluation with sufficient evidence, including documentation. If the auditor concludes that management has not fulfilled these responsibilities, Auditing Standard No. 2 states that the auditor should communicate, in writing, to management and the audit committee that the audit of internal control over financial reporting cannot be satisfactorily completed and that he or she is required to disclaim an opinion. Therefore, an auditor could not render either an adverse opinion on management's assessment or an unqualified opinion on internal control over financial reporting because, in this situation, the auditor would be precluded from expressing any opinion.

Additionally, management is required to fulfill these responsibilities under Items 308(a) and (c) of Regulation S-B and S-K, 17 C.F.R. 228.308 (a) and (c) and 229.308 (a) and (c), respectively. To the extent that management has willfully decided not to fulfill these responsibilities, the auditor also may have responsibilities under AU sec. 317, *Illegal Acts by Clients,*[1/] and Section 10A of the Securities Exchange Act of 1934.

Q9. Is it necessary for the auditor to test controls directly if management asserts that internal control over financial reporting is ineffective? If the auditor identifies a material weakness, does the auditor need to complete his or her testing of controls?

A9. Yes. Paragraph 27 of Auditing Standard No. 2 requires the auditor to obtain sufficient competent evidence about the design and operating

---

[1/] The Board adopted the generally accepted auditing standards, as described in the AICPA Auditing Standards Board's ("ASB") Statement on Auditing Standards No. 95, *Generally Accepted Auditing Standards,* as in existence on April 16, 2003, on an initial, transitional basis. The Statements on Auditing Standards promulgated by the ASB have been codified into the AICPA *Professional Standards*, Volume 1, as AU sections 100 through 900. References in Auditing Standard No. 2 and this Staff Questions and Answers document refer to those generally accepted auditing standards, as adopted on an interim basis in PCAOB Rule 3200T.

effectiveness of controls over all relevant financial statement assertions related to all significant accounts and disclosures in the financial statements. That paragraph also requires the auditor to plan and perform the audit to obtain reasonable assurance that *all* material weaknesses are identified. Therefore, to complete an audit of internal control over financial reporting and render an opinion, it is necessary for the auditor to test controls directly, regardless of the company's assessment or the auditor's earlier identification of a material weakness.

Q10. Auditing Standard No. 2 describes five financial statement assertions and describes the auditor's responsibilities in terms of relevant assertions. Some professional standards, such as the International Standards on Auditing, include more than five financial statement assertions. Some companies are using fewer than five assertions when making their assessments. For the auditor to perform an audit of internal control over financial reporting in accordance with Auditing Standard No. 2, must management and the auditor use the five assertions described therein?

A10. No. For the auditor to perform an audit of internal control over financial reporting in accordance with Auditing Standard No. 2, management and the auditor may base their evaluations on assertions that are different from those specified in Auditing Standard No. 2. Paragraphs 69 and 70 of Auditing Standard No. 2 describe the identification of relevant assertions. Relevant assertions are those that have a meaningful bearing on whether the account is fairly stated. To identify relevant assertions, the auditor should determine the sources of likely potential misstatements in each significant account. Ultimately, management and the auditor should identify and test controls over all relevant assertions for all significant accounts. To the extent that management or the auditor bases his or her work on assertions different from those in Auditing Standard No. 2, the auditor would be required to determine that he or she had identified and tested controls over all sources of likely potential misstatements in each significant account and over all representations by management that have a meaningful bearing on whether the account is fairly stated.

Evaluating Deficiencies

Q11. The definition of a significant deficiency is based, in part, on a magnitude of financial statement misstatement that is "more than inconsequential." Paragraphs E87-

STAFF QUESTIONS & ANSWERS

E91 of Auditing Standard No. 2 describe the development of the Board's definition of the term *inconsequential*. The definition is based on paragraph .41 of AU sec. 312, *Audit Risk and Materiality in Conducting an Audit*, which states:

> In aggregating likely misstatements that the entity has not corrected, pursuant to paragraphs .34 and .35 [of AU sec. 312], the auditor may designate an amount below which misstatements need not be accumulated. This amount should be set so that any such misstatements, either individually or when aggregated with other such misstatements, would not be material to the financial statements, after the possibility of further undetected misstatements is considered.

In the audit of the financial statements, different auditors designate the amount described in paragraph .41 of AU sec. 312 in various ways. Some auditors quantify, during the planning phase of the audit, a specific dollar amount above which likely misstatements will be accumulated. Others take a more judgmental approach to determining which likely misstatements to accumulate. Of the auditors who quantify a specific dollar amount above which likely misstatements will be accumulated, different auditors use different methodologies to arrive at different thresholds or specific dollar amounts.

Given the relationship of paragraph .41 of AU sec. 312 to the definition of inconsequential, is a known or likely misstatement aggregated by the auditor during the audit of the financial statements in response to the directions in paragraph .41 of AU sec. 312 by definition "more than inconsequential"? Furthermore, by virtue of having been aggregated by the auditor, such a misstatement would have a "more than remote likelihood" of occurring; therefore, by extension, does the aggregation of a difference by the auditor, by definition, mean that there is a significant deficiency in the company's internal control over financial reporting?

> **A11.** No. A known or likely misstatement aggregated by the auditor as part of the audit of the financial statements is not, by definition, either "more than inconsequential" or determinative of there being a significant deficiency. There are several reasons and circumstances why such a likely misstatement aggregated by the auditor might or might not indicate the existence of a significant deficiency.

STAFF QUESTIONS & ANSWERS

The threshold for "more than inconsequential" when evaluating whether a significant deficiency exists is not necessarily the same as the amount the auditor establishes pursuant to paragraph .41 of AU section 312 for aggregating misstatements. The definition of inconsequential includes a combination of concepts from both Staff Accounting Bulletin ("SAB") No. 99, *Materiality*, and AU sec. 312. The definition of inconsequential is largely based on the discussion of magnitude in SAB No. 99 and on AU sec. 312 for its directions regarding both the consideration of misstatements individually and in the aggregate as well as the possibility of undetected misstatements.

Also, as the Board indicated in paragraph E75 of the Background and Basis for Conclusions of Auditing Standard No. 2, one reason that a significant deficiency is defined differently from the previously used term "reportable condition" is because the definition of reportable condition was solely a matter of the auditor's judgment. A definition dependent *solely* on the auditor's judgment was insufficient for purposes of the Sarbanes-Oxley Act because management also needs a definition to determine whether a deficiency is significant, and that definition should be the same as the definition used by the auditor. Accordingly, Auditing Standard No. 2's definition of significant deficiency is not, by definition, the same as the auditor's threshold for aggregating likely misstatements in the audit of the financial statements.

As indicated in the question, different auditors exercise their professional judgment in different ways in different circumstances when accumulating likely misstatements as part of the audit of the financial statements. Furthermore, some auditors, as a matter of policy, tend to set their posting threshold for accumulating likely misstatements lower than "inconsequential." For example, some auditors set their posting threshold for accumulating likely misstatements at .0025 percent of the company's pre-tax income which would, in most cases, be clearly inconsequential on a quantitative basis.

Because a likely misstatement aggregated by the auditor as part of the audit of the financial statements is not, by definition, "more than inconsequential" or determinative of the existence of a significant deficiency, the auditor need not align the amount above which he or she aggregates misstatements with the amount above which he or she believes a misstatement to be "more than inconsequential" or determinative of the existence of a significant deficiency.

STAFF QUESTIONS & ANSWERS

Furthermore, the auditor should not, for example, change the types of deficiencies that he or she determines to be significant deficiencies simply by raising the auditor's threshold for accumulating likely misstatements. These determinations also need to take into consideration qualitative, as well as quantitative, factors. The auditor might still determine that there is a more than remote likelihood that a misstatement *larger* than the difference on his or her summary of audit differences might occur and not be prevented or detected. For these reasons, it is possible that a control deficiency associated with a likely misstatement accumulated by the auditor on his or her summary of audit differences might indicate the existence of a deficiency, a significant deficiency, *or* a material weakness.

Q12. When determining whether a control deficiency exists, should the auditor consider compensating controls?

A12. No. The Note to paragraph 10 of Auditing Standard No. 2 states that "… in determining whether a control deficiency or combination of deficiencies is a significant deficiency or a material weakness, the auditor should evaluate the effect of compensating controls and whether such compensating controls are effective." An important part of the evaluation of whether a significant deficiency or material weakness exists includes aggregating deficiencies and considering their effect in combination. The logical extension of this aggregation is to also consider compensating controls. However, control deficiencies should be considered individually and in isolation; therefore, the existence of compensating controls does not affect whether a control deficiency exists.

Q13. Are all control testing exceptions, by definition, control deficiencies?

A13. No. Paragraph 107 of Auditing Standard No. 2 states: "A conclusion that an identified exception does not represent a control deficiency is appropriate only if evidence beyond what the auditor had initially planned and beyond inquiry supports that conclusion." Paragraph 133 also includes the example that "a control with an observed non-negligible deviation rate is a deficiency." Both these passages in the standard recognize the inherent limitations in internal control. Effective internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting. Because effective internal control over financial reporting cannot, and does not,

STAFF QUESTIONS & ANSWERS

provide absolute assurance of achieving financial reporting objectives, any individual control does not necessarily have to operate perfectly, all the time, to be considered effective. Therefore, Auditing Standard No. 2 provides the auditor with directions that allow the use of judgment in the circumstances in which he or she is evaluating whether a control testing exception is a control deficiency.

Q14. When a control deficiency exists, what degree of precision is required for a compensating control to effectively mitigate a significant deficiency or material weakness?

A14. As discussed in A13, Auditing Standard No. 2 provides that auditors should evaluate the effect of compensating controls when determining whether a control deficiency or combination of deficiencies is a significant deficiency or a material weakness. However, to have a mitigating effect, the compensating control should operate at a level of precision that would prevent or detect a misstatement that was more than inconsequential or material, respectively.

Q15. Paragraph 9 of Auditing Standard No. 2 defines a significant deficiency as "a control deficiency, or combination of control deficiencies ..." Paragraph 10 defines a material weakness as "a significant deficiency, or combination of significant deficiencies..." The definition of a material weakness, therefore, relies on the definition of significant deficiency. Does this mean that a control deficiency, once determined to be only a control deficiency and not also a significant deficiency, could be excluded from the evaluation of whether a significant deficiency or combination of significant deficiencies constitutes a material weakness?

A15. No. The definitions of significant deficiency and material weakness delineate increasingly severe types of control deficiencies. All significant deficiencies are also deficiencies; all material weaknesses are also significant deficiencies and deficiencies. If the auditor correctly aggregates control deficiencies when evaluating whether a significant deficiency exists, then all related and salient control deficiencies will also be included in the auditor's evaluation of whether a combination of significant deficiencies represents a material weakness. Therefore, whether the definition of a material weakness is expressed as "a significant deficiency, or combination of significant deficiencies…" or as "a control deficiency, or combination of control

STAFF QUESTIONS & ANSWERS

deficiencies…" is unimportant. Both the meaning and the evaluation are the same.

Multi-Location Issues

Q16. Paragraph 87 of Auditing Standard No. 2 states:

> Appendix B, paragraphs B1 through B17, provide additional direction to the auditor in determining which controls to test when a company has multiple locations or business units. In these circumstances, the auditor should determine significant accounts and their relevant assertions, significant processes, and major classes of transactions based on those that are relevant and significant to the consolidated financial statements. Having made those determinations in relation to the consolidated financial statements, the auditor should then apply the directions in Appendix B.

Paragraph B4 states:

> Because of the importance of financially significant locations or business units, the auditor should evaluate management's documentation of and perform tests of controls over all relevant assertions related to significant accounts and disclosures at each financially significant location or business unit, as discussed in paragraphs 83 through 105 [of the standard].

Does the combination of these directions mean that, for example, if the auditor determines that accounts receivable is a significant account to the consolidated financial statements, the auditor should test controls over all relevant assertions over accounts receivable at every financially significant location or business unit, even if accounts receivable at a particular financially significant location is immaterial?

> **A16.** No. The combination of these directions means that the auditor should determine significant accounts and their relevant assertions based on the consolidated financial statements and perform tests of controls over all relevant assertions related to those significant accounts at each financially significant location or business unit for which the selected accounts are material at the account level. Therefore, the auditor need not test controls over all relevant

STAFF QUESTIONS & ANSWERS

assertions for a significant account at a financially significant location where the significant account is immaterial. However, if accounts receivable is material at a location or business unit that is not otherwise considered financially significant, the auditor should test controls over all relevant assertions for accounts receivable at that location. This direction is consistent with the directions in paragraph B6 addressing locations or business units that involve specific risks.

Q17. The multi-location guidance in Appendix B of Auditing Standard No. 2 states that the auditor should test controls over a "large portion" of the company's operations and financial position. Many auditors are referring to specific percentages that represent coverage over a "large portion" of the company's operations and financial position, such as 60 percent or 75 percent. Are these percentages set in Auditing Standard No. 2?

A17. No. Auditing Standard No. 2 does not establish specific percentages that would achieve this level of testing. During the comment period on the proposed standard for the audit of internal control over financial reporting, several commenters suggested that the standard should provide more specific directions regarding the evaluation of whether controls over a "large portion" of the company's operations and financial position had been tested, including establishing specific percentages. The Board decided that balancing auditor judgment with the consistency that would be enforced by increased specificity would be best served by this direction remaining "principles-based." Therefore, Auditing Standard No. 2 leaves to the auditor's judgment the determination of what exactly constitutes a "large portion."

Additionally, the Note to paragraph B11 states that, "the evaluation of whether controls over a large portion of the company's operations or financial position have been tested should be made at the overall level, not at the individual significant account level." For example, if an auditor believes that he or she should test controls over x percent of some measure, that auditor should evaluate whether he or she had tested controls over x percent of the company's consolidated operations or financial position (e.g., x percent of total assets or x percent of revenues) and not x percent of each individual significant account.

Q18. Is any type of sampling strategy accommodated by the direction to test controls over "a large portion" of financial position or operations?

STAFF QUESTIONS & ANSWERS

A18. Yes. The directions in paragraph B11 of Auditing Standard No. 2 that the auditor should test controls over a large portion of the company's operations or financial position are intended as a fail-safe to ensure that every audit of internal control over financial reporting is supported by sufficient evidence. In no case should the auditor find that, in following the directions in paragraphs B1-B10, the auditor could merely test company-level controls without also testing controls over all relevant assertions related to significant accounts and disclosures.

The direction to test controls over a large portion of financial position or operations is easily satisfied at companies in which the auditor's testing of individual financially significant locations or business units clearly covers a large portion. At these types of entities and others, the type of judgment discussed in Q17 in which an auditor determines that he or she should test controls over 60 percent or 75 percent of the company's financial position or operations are readily satisfied. However, in circumstances in which a company has a very large number of individually insignificant locations or business units, testing controls over 60 percent or 75 percent of the company's financial position or operations may result in an extensive amount of work, in which the auditor would test controls over hundreds and even thousands of individual locations to reach that type of percentage target. In circumstances in which a company has a very large number of individually insignificant locations or business units and management asserts to the auditor that controls have been documented and are effective at all locations or business units, the auditor may satisfy the directions in paragraph B11 by testing a representative sample of the company's locations or business units.

The auditor may select the representative sample either statistically or non-statistically. However, the locations or business units should be selected in such a way that the sample is expected to be representative of the entire population. Also, particularly in the case of a non-statistical sample, the auditor's sampling will be based on the expectation of no, or very few, control testing exceptions. In such circumstances, because of the nature of the sample and the control testing involved, the auditor will not have an accurate basis upon which to extrapolate an error or exception rate that is more than negligible. Furthermore, the existence of testing exceptions would not support management's assertion that controls had been documented and were effective at all locations or business units. Therefore, if the auditor elects to use a representative sample in these

STAFF QUESTIONS & ANSWERS

circumstances and encounters testing exceptions within the sample that exceed a negligible rate, the auditor might decide that testing controls over a very large number of individual locations or business units is necessary to adequately support his or her opinion.

Q19. Paragraphs B16 and B17 of Auditing Standard No. 2 provide direction to the auditor in situations in which the SEC allows management to limit its assessment of internal control over financial reporting by excluding certain entities. The SEC staff's guidance, *Office of the Chief Accountant and Division of Corporation Finance: Management's Report on Internal Control Over Financial Reporting and Disclosure in Exchange Act Periodic Reports, Frequently Asked Questions*, dated June 23, 2004, discusses such situations in Questions 1 and 3. However, that document also instructs management to refer in its report on internal control over financial reporting to disclosure in its Form 10-K or Form 10-KSB regarding the scope of management's assessment and any entity excluded from the scope. How does this disclosure by management in its report affect the directions in Auditing Standard No. 2 that instruct the auditor, in these situations, to report without reference to the limitation in scope?

A19. In these situations, the auditor's opinion would not be affected by a scope limitation. However, the auditor should include, either in an additional explanatory paragraph or as part of the scope paragraph in his or her report, a disclosure similar to management's regarding the exclusion of an entity from the scope of both management's assessment and the auditor's audit of internal control over financial reporting.

Using the Work of Others

Q20. Auditing Standard No. 2 allows the auditor to use the work of others to alter the nature, timing, or extent of the work the auditor would otherwise have performed. If the auditor plans to use the work of others, he or she should, among other things, test some of the work performed by others to evaluate the quality and effectiveness of the work. In performing this testing, does the auditor need to test the work of others in every significant account in which the auditor plans to use their work?

A20. No. Auditing Standard No. 2 establishes a framework for using the work of others based on evaluating the nature of the controls, evaluating the competence and objectivity of the individuals who performed the work, and

STAFF QUESTIONS & ANSWERS

testing some of the work performed by others to evaluate the quality and effectiveness of their work. Within this framework, the amount of testing of the work of others should be sufficient to enable the auditor to evaluate the overall quality and effectiveness of their work. Auditing Standard No. 2 provides flexibility in this regard; testing the work of others in every significant account in which the auditor plans to use their work is not required. Furthermore, if the auditor believes that extensive testing of the work of others is necessary in every area in which the auditor plans to use their work, the auditor should keep in mind the directions in paragraph 124 of Auditing Standard No. 2. Those directions state that the auditor should also assess whether the evaluation of the quality and effectiveness of the work of others has an effect on the auditor's conclusions about the competence and objectivity of the individuals performing the work. If the auditor determines the need to test the work of others to a high degree, the auditor should consider whether his or her original assessment of their competence and objectivity is correct.

Q21. Paragraph 108 of Auditing Standard No. 2 requires the auditor to perform enough of the testing himself or herself so that the auditor's own work provides the principal evidence for the auditor's opinion. Does the auditor's testing of the work of others "count" toward the auditor obtaining the principal evidence supporting his or her opinion?

A21. No. As described in paragraph 109 of Auditing Standard No. 2, to determine the extent to which the auditor may use the work of others to alter the nature, timing, or extent of the work the auditor would have otherwise performed, *in addition to obtaining the principal evidence for his or her opinion*, the auditor should, among other things, test some of the work performed by others to evaluate the quality and effectiveness of their work. Therefore, the auditor's testing of the work of others is not considered to be part of the principal evidence obtained by the auditor. As described in A20, if the auditor determines the need to test the work of others to a high degree, the auditor should consider whether his or her original assessment of their competence and objectivity is correct.

Q22. Paragraph 123 of Auditing Standard No. 2 states that the auditor's tests of the work of others may be accomplished by either (a) testing some of the controls that others tested or (b) testing similar controls not actually tested by others. Based on the response in A21, regardless of whether the auditor tested some of the controls tested

STAFF QUESTIONS & ANSWERS

by others or tested similar controls not actually tested by others ("independent testing"), if the objective of that testing is to evaluate the quality and effectiveness of the work of others, that testing should not be considered as part of the principal evidence obtained by the auditor. However, does the auditor's independent testing in areas in which the auditor is using the work of others count as principal evidence if the independent tests are not for the purpose of assessing the quality and effectiveness of the work of others?

> **A22.** Yes. The auditor's independent testing in these circumstances may be considered as work performed by the auditor when evaluating whether the auditor obtained the principal evidence supporting his or her opinion, but only if these independent tests are not for the purpose of assessing the quality and effectiveness of the work of others. If the independent tests are for the purpose of assessing the quality and effectiveness of the work of others, then the independent tests should not be considered as work performed by the auditor when evaluating whether the auditor obtained the principal evidence supporting his or her opinion.

Q23. Paragraphs 113 through 115 of Auditing Standard No. 2 describe the auditor's evaluation of the nature of the controls subjected to the work of others when determining how to use the work of others to alter the nature, timing, or extent of the work the auditor would otherwise have performed. Those paragraphs state that the auditor should not use the work of others to reduce the amount of work he or she performs on controls in the control environment. Further, those directions state that controls that are part of the control environment include, but are not limited to, controls specifically established to prevent and detect fraud that is at least reasonably possible to result in a material misstatement of the financial statements. How do these directions regarding the auditor's testing of controls specifically established to prevent and detect fraud relate to the auditor's responsibilities in AU sec. 316, *Consideration of Fraud in a Financial Statement Audit*?

> **A23.** Paragraph 26 of Auditing Standard No. 2 generally describes how the auditor's evaluation of controls in an audit of internal control over financial reporting is interrelated with the auditor's evaluation of fraud risks in a financial statement audit as required by AU sec. 316. AU sec. 316 requires, among other things, that the auditor identify risks that may result in a material misstatement of the financial statements due to fraud and that the auditor should respond to those identified risks. AU sec. 316 emphasizes that the auditor's response to the risks

STAFF QUESTIONS & ANSWERS

of material misstatement due to fraud involves the application of professional skepticism when gathering and evaluating evidence. The auditor also is required to respond to the results of the fraud risk assessment in three ways:

a. A response that has an overall effect on how the audit of the financial statements is conducted, that is, a response involving more general considerations apart from the specific procedures otherwise planned.

b. A response to identified risks that involves the nature, timing, and extent of auditing procedures to be performed.

c. A response involving the performance of certain procedures to further address the risk of material misstatement due to fraud involving management override of controls.

The relationship of these requirements with the directions in Auditing Standard No. 2 regarding the auditor's use of the work of others may be illustrated by several examples.

First, AU sec. 316 establishes a presumption that there is a risk of material misstatement due to fraud relating to revenue recognition. If the auditor does not overcome this presumption, as would frequently be the case with, for example, software revenue recognition, the auditor should test the controls specifically established to prevent and detect fraud related to a material misstatement of the company's revenue recognition himself or herself.

Because material misstatement due to fraud often involves manipulation of the financial reporting process by management, AU sec. 316 also requires the auditor to review journal entries and other adjustments for evidence of material misstatement due to fraud. Paragraph 112 of Auditing Standard No. 2 includes as one of the factors that the auditor should evaluate when evaluating the nature of the controls subjected to the work of others "the potential for management override of the control." Taken together, these directions mean that obtaining the understanding of the design of controls over journal entries and other adjustments and determining whether they are suitably designed and have been placed in operation, as required by AU sec. 316, and performing any associated

STAFF QUESTIONS & ANSWERS

testing of those controls that the auditor determines is necessary when auditing internal control over financial reporting under Auditing Standard No. 2, should be performed by the auditor himself or herself. However, Auditing Standard No. 2 emphasizes that, although the auditor should not use the work of others in this situation, the auditor should consider the results of work performed in the area by others because it might indicate the need for the auditor to increase his or her work.

Service Organizations

Q24. What types of outsourcing activities result in a service organization arrangement addressed by Statement on Auditing Standards ("SAS") No. 70, *Service Organizations* (AU sec. 324)? What types of outsourcing activities are part of a company's internal control over financial reporting?

A24. As described in paragraph .03 of AU sec. 324, a service organization's services are part of a company's information system if they affect any of the following:

- The classes of transactions in the company's operations that are significant to the company's financial statements.
- The procedures, both automated and manual, by which the company's transactions are initiated, authorized, recorded, processed, and reported from their incurrence to their inclusion in the financial statements.
- The related accounting records, whether electronic or manual, supporting information and specific accounts in the company's financial statements involved in initiating, authorizing, recording, processing and reporting the company's transactions.
- How the company's information system captures other events and conditions that are significant to the financial statements.

STAFF QUESTIONS & ANSWERS

- The financial reporting process used to prepare the company's financial statements, including significant accounting estimates and disclosures.

Paragraph .03 of AU sec. 324 also provides examples of situations in which a service organization's services affect a company's information system. For instance, the trust departments of banks and insurance companies often serve as the custodian of an employee benefit plan's assets, including making investment decisions, maintaining records of each participants account, allocating income amongst participants, and preparing other types of recordkeeping; this type of servicing is a common example of a service organization's services that affect a company's information system. In contrast, AU sec. 324 does not apply to situations in which the services being provided are limited to executing client organization transactions that the client specifically authorizes. For example, the processing of checking account transactions or wire transfer instructions by a bank would not constitute a service organization arrangement. Paragraph .03 of AU sec. 324 also excludes other types of transactions, such as transactions arising from joint ventures, from the scope of a service organization arrangement addressed by AU sec. 324.

All of the examples of outsourcing activities in paragraph .03 of AU sec. 324 (which are not an exhaustive listing of all types of possible outsourcing activities) are part of the company's information system. However, not all outsourcing activities are a part of the company's information system. In addition to the arrangements described in paragraph .03 of AU sec. 324 to which AU sec. 324 does *not* apply, the use of a specialist is not part of a company's information system. For example, a company might outsource actuarial services; however, the nature of the services represents the use of a specialist, and the actuary is not a part of the company's information system.

If the service organization's services are part of a company's information system, then they are part of the information and communication component of the company's internal control over financial reporting. In those circumstances, management should consider the activities of the service organization in making its assessment of internal control over financial reporting, and the auditor should consider the activities of the service organization in determining the evidence required to support his or her opinion. Appendix B of Auditing Standard No. 2

STAFF QUESTIONS & ANSWERS

provides additional directions regarding the procedures management and the auditor should perform with respect to activities performed by the service organization.

Q25. Auditing Standard No. 2 indicates that evidence about the operating effectiveness of controls at a service organization can be obtained from a Type 2 SAS No. 70 report. Is a Type 2 SAS No. 70 report issued more than six months prior to the date of management's assessment current enough to provide any such evidence?

A25. Paragraphs B25 through B27 provide directions when a significant period of time has elapsed between the time period covered by the tests of controls in the service auditor's report and the date of management's assessment. These directions do not establish any "bright lines." In other words, application of the directions does not result in a precise answer as to whether a service auditor's report issued more than six months prior to the date of management's assessment is not current enough to provide *any* evidence. Rather, these directions state that, when a significant period of time has elapsed between the time period covered by the tests of controls in the service auditor's report and the date of management's assessment, additional procedures should be performed.

Paragraph B26 provides directions to the auditor in determining whether to obtain additional evidence about the operating effectiveness of controls at the service organization. The auditor's procedures to obtain additional evidence will typically be more extensive the longer the period of time that has elapsed between the time period covered by the service auditor's report and the date of management's assessment. Also, those auditor's procedures will vary depending on the importance of the controls at the service organization to management's assessment and on the level of interaction between the company's controls and the controls at the service organization.

The auditor's procedures will be focused on, among other things, identifying changes in the service organization's controls subsequent to the period covered by the service auditor's report. The auditor should be alert for situations in which management has not made changes to its procedures and controls to respond to changes in procedures and controls at the service organization. These situations might result in errors not being prevented or detected in a timely manner.

STAFF QUESTIONS & ANSWERS

Q26. Can a registered public accounting firm in the integrated audit of an issuer obtain evidence from a service auditor's report issued by a non-registered public accounting firm?

A26. Yes. Paragraph B24 of Auditing Standard No. 2 directs the auditor to make inquiries concerning the service auditor's reputation, competence, and independence in determining whether the service auditor's report provides sufficient evidence to support management's assessment and the auditor's opinion on internal control over financial reporting. Auditing Standard No. 2 does not require that the service auditor be a registered public accounting firm.

The auditor should be aware of how evidence obtained from a service auditor's report issued by a non-registered firm interacts with the Board's registration rules. Any public accounting firm that "plays a substantial role in the preparation or furnishing of an audit report" with respect to any issuer must register with the Board. Because of the nature of the service auditor's report (the user auditor could have performed tests of controls at the service organization himself or herself but, instead, may have chosen to obtain evidence from a service auditor's report), when a registered public accounting firm obtains evidence from a service auditor's report in the audit of an issuer, the service auditor has participated in the audit of the issuer. If the service auditor's work, measured in terms of either services or procedures, meets the "substantial role" threshold (as defined in Rule 1001(p)(ii)) for the audit of the user organization, the service auditor is required to be registered with the Board.

Index of Frequently Asked Questions

Index of Lessons Learned

PricewaterhouseCoopers (www.pwc.com) provides industry-focused assurance, tax and advisory services for public and private clients. More than 120,000 people in 139 countries connect their thinking, experience and solutions to build public trust and enhance value for clients and their stakeholders.

"PricewaterhouseCoopers" refers to the network of member firms of PricewaterhouseCoopers International Limited, each of which is a separate and independent legal entity.

NY-FP-04-1492-A

us.pwc.com